Algebraiska strukturer, 21 januari

MÄNGDER OCH OPERATIONER

De fyra räknesätten: addition, subtraktion, multiplikation och division är, vad man ofta kallar, (aritmetiska) operationer i mängder av alla tal.

Definition. Låt M vara en mängd. En **binär operation** $*$ på M är en regel som till varje ordnat par (x, y) av element i M ordnar ett nytt element i M. Detta nya element skriver vi $x * y$.

$$(x, y) \mapsto x * y \in M$$

Definitionen säger att en binär operation är en funktion från kartesianska produkten $M \times M = \{(x, y) \mid x, y \in M\}$ till M.

Exempel 1. (a) Låt M vara en av mängderna $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ och låt $a * b = a + b$, $(a, b) \mapsto a + b$

(b) $M = \mathbb{N}$, $m * n = m^n$, $(m, n) \mapsto m^n \in \mathbb{N}$.

(c) $M = \mathbb{Z}$, $m * n = m - n$. (Obs! $*$ - ej operation på $\mathbb{N}$, ty, t.ex., $2 * 3 = 2 - 3 \notin \mathbb{N}$).

(d) Låt M vara mängden av (2×2)-matriser med reella element och $A * B = AB$, den vanliga matrisprodukten för A, $B \in Mat_2(\mathbb{R})$.

Om $M = \{a_1, a_2, \ldots, a_n\}$ är en ändlig mängd så definierar man ofta operationer på M m h a "multiplikationstabeller" (Cayleytabeller):

$*$	a_1	$\ldots$	a_i	$\ldots$	a_j	$\ldots$	a_n
a_1	$a_1 * a_1$	$\ldots$	$a_1 * a_i$	$\ldots$	$a_1 * a_j$	$\ldots$	$a_1 * a_n$
$\vdots$		$\ddots$					
a_i	$a_i * a_1$	$\ldots$	$a_i * a_i$	$\ldots$	$a_i * a_j$	$\ldots$	$a_i * a_n$
$\vdots$				$\ddots$			
a_j	$a_j * a_1$	$\ldots$	$a_j * a_i$	$\ldots$	$a_j * a_j$	$\ldots$	$a_j * a_n$
$\vdots$						$\ddots$	
a_n	$a_n * a_1$	$\ldots$	$a_n * a_i$	$\ldots$	$a_n * a_j$	$\ldots$	$a_n * a_n$

Exempel 2. Låt $M = \{-1, 1\}$, $*$ är en vanlig multiplikation. Multiplikationstabellen för $*$ blir då

$*$	1	-1
1	1	-1
-1	-1	1

Definition. En operation $*$ på M kallas **kommutativ** om $a*b = b*a$ för alla $a, b \in M$. Den kallas **associativ** om $a*(b*c) = (a*b)*c$ då a, b, $c \in M$. Man säger att $e \in M$ är ett **neutralt element** för $*$ om $a*e = e*a = a$ då $a \in M$.

Exempel 3. (a) De vanliga additionen och multiplikationen är kommutativa och associativa på $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$.

(b) Betrakta $(\mathbb{N}, *)$, där $m*n = m^n$. $*$ är inte kommutativ, ty t.ex $2*3 = 2^3 = 8 \neq 3^2 = 3*2$, den är inte associativ heller, ty t.ex. $2*(2*3) = 2*2^3 = 2^{2^3} = 2^8$, men $(2*2)*3 = 2^2*3 = (2^2)^3 = 2^6$.

Med hjälp av multiplikationstabellen kan man lätt avgöra om operationen är kommutativ (Hur?), har ett neutralt element (Hur?).

Obs! Att kontrollera att operationen är associativ är inte lika lätt!!

GRUPPER

Definition. Låt G vara en mängd och låt $*$ vara en operation på G dvs

(0) $a * b \in G$ då $a, b \in G$ (sluthet).

Man säger att $(G, *)$ är en **grupp** om

(1) $*$ är associativ, dvs $(a * b) * c = a * (b * c)$, då $a, b, c \in G$;

(2) det finns $e \in G$ så att $e * a = a * e = a$ då $a \in G$ (neutralt element eller identiteselement),

(3) till varje $a \in G$ ska det finnas ett element $a' \in G$ så att $a' * a = a * a' = e$ (invers)

Vi skriver $(G, *)$. Det följer från Sats 5.1 att i varje grupp finns det endast ett neutralt element (identitetselement) och varje gruppelement a har endast en invers a'.

Exempel 4. (a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ med operationen $+$ är grupper (ej $\mathbb{N}$)

(b) Om vi utelämnar 0 ur $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ får vi grupper med avseende på den vanliga multiplikationen ($(\mathbb{Z} \setminus \{0\}, \cdot)$ är inte en grupp).

(c) Låt X vara en mängd och låt G bestå av bijektiva funktioner. Operationen $*$ är sammansättningen av två funktioner: $(f * g)(x) = f(g(x))$. $(G, *)$ är en grupp (Visa!)

(d) Låt G bestå av rotationer och speglingar av planet som överför n-höringen på sig själv och låt $*$ vara sammansättningen. $(G, *)$ är en grupp.

Sats 5.1. I varje grupp finns det endast ett neutralt element e och varje gruppelement a har endast en invers a'.

Bevis. 1. Låt e och f vara element i G som uppfyller

$$a * e = e * a = a \text{ då } a \in G \tag{1}$$

$$a * f = f * a = a \text{ då } a \in G \tag{2}$$

Då gäller $f =$ (enligt (1) $= e * f =$ (enligt (2)) $= e$, dvs $f = e$.

2. Låt $a \in G$ och låt $b, c \in G$ uppfylla

$$a * b = b * a = e \text{ och } a * c = c * a = e,$$

(e är det neutrala elementet). Då gäller

$$b = b * e = b * (a * c) = (\text{assoc}) = (b * a) * c = e * c = c,$$

dvs $b = c$.

Inversen till $a \in G$ betecknar man ofta a^{-1}.

Anmärkning. (a) När man definierar en grupp så beskriver man mängden G av dess element och gruppoperationen $*$. Formellt borde man säga att $(G, *)$ är en grupp. Icke-desto mindre säger man oftast att G är en grupp.

(b) Vi vet redan att symbolen "$*$" som betecknar en operation kan tolkas på olika sätt. När det gäller beteckningar finns det två

vanliga typer som dels beror på traditionen dels på bekvämligheten. Det är säkert bekvämare att skriva ab eller $a \cdot b$ i stället för $a * b$. Då säger man om **multiplikativ notation**. Inversen betecknas då med a^{-1}. Ibland är denna notation inte helt naturlig, speciellt när gruppoperationen är addition. Då använder man **additiv notation** dvs man tolkar "$*$" som "$+$". Inversen betecknas då med $-a$ och identitetselementet med 0.

Proposition. Låt G vara en grupp och a, b, $c \in G$. Då gäller strykningarna

$$(a) \quad a * c = b * c \Rightarrow a = b$$
$$(b) \quad c * a = c * b \Rightarrow a = b$$

Bevis. (a) Multiplicera från höger med inversen c^{-1} till c. Enligt associativiteten får vi

$$\begin{aligned}(a * c) * c^{-1} = (b * c) * c^{-1} &\Leftrightarrow a * (c * c^{-1}) = b * (c * c^{-1}) \\ &\Leftrightarrow a * e = b * e \Leftrightarrow a = b.\end{aligned}$$

Cayleytabell. Låt $G = \{a_1, \ldots, a_n\}$ vara en ändlig mängd. Varje operation på G kan beskrivas m h a Cayleytabell. Cayleytabellen för en grupp har följande egenskap: Varje element förekommer precis en gång i varje rad och precis en gång i varje kolonn, ty en rad i tabellen består av produkterna $a_i * a_1, \ldots, a_i * a_j, \ldots, a_i * a_n$, alla dessa produkter ger olika element i G därför att $a_i * a_j = a_i * a_k$ ger $a_j = a_k$. I almänhet är det inte lätt avgöra om en operation på G definierar en grupp genom att studera Cayleytabellen. Genom inspektion av denna upptäcker man lätt om det finns ett neutralt element (Hur?) och om varje element har en invers (varje rad och varje kolonn måste innehålla det neutrala elementet). Associativiteten är svårt att kontrollera.

Algebraiska strukturer, 23 januari

PERMUTATIONER

Definition. En **permutation** av en mängd S är en bijektiv funktion $\sigma : S \to S$. Mängden av alla permutationer bildar en grupp $Sym(S)$ under sammansättningen (se exempel 4 (c)). Om $S = \{1, 2, \ldots, n\}$ betecknar man $Sym(S)$ med S_n. För att beskriva elementen i S_n använder man tabellbeteckningen:

Om $\sigma(1) = a_1$, $\sigma(2) = a_2, \ldots, \sigma(n) = a_n$ kommer vi att skriva

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

Antalet element i S_n är $n!$

Permutationer kan presenteras mera kompakt. Låt $p_1, p_2, \ldots, p_k \in \{1, 2, \ldots, n\}$ och låt $(p_1, p_2, \ldots, p_k)$ beteckna funktionen $\sigma(p_1) = p_2$, $\sigma(p_2) = p_3, \ldots, \sigma(p_k) = p_1$ och $\sigma(i) = i$, då $i \neq p_1, \ldots, p_k$. T.ex. $(1, 2, 3)$ är beteckningen på $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

$(p_1, p_2, \ldots, p_k)$ kallas för en **cykel av längd** k.

Om $f = (p_1, p_2, \ldots, p_k)$ och $g = (p'_1, p'_2, \ldots, p'_k)$, där alla tal $p_1, p_2, \ldots, p_k, p'_1, p'_2, \ldots, p'_k$ är olika då säger man att f och g är disjunkta cykler.

För två disjunkta cykler $\rho, \sigma \in S_n$ gäller att $\rho\sigma = \sigma\rho$. Visa!

Varje permutation kan skrivas som en produkt av disjunkta cykler. Här följer ett enkelt recept: Man väljer ett tal p_1 som inte avbildas på sig självt. Därefter tar man bilden p_2 av p_1, bilden p_3 av p_2 osv tills man får p_1 igen. Då har man en cykel. Nu tar vi ett tal som inte ingår i första cykel och gör på samma sätt. T.ex. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix} = (1, 4, 6)(2, 3)(5) = (1, 4, 6)(2, 3)$. Man brukar utelämna cykler av längd 1.

En cykel (a, b) av längd 2 kallas för **transposition**. En transposition byter alltså plats på två element och låter övriga vara.

Påstående. Varje permutation i S_n, $n \geq 2$, kan skrivas som en produkt av transpositioner.

Bevis. Övning 6.9 i kursboken.

En permutation i S_n, $n \geq 2$ kan skrivas som en produkt av antingen ett jämnt eller udda antal transpositioner.

En permutation i S_n kallas **jämn** eller **udda**, beroende på om den kan skrivas som ett jämnt eller udda antal transpositioner.

Exempel. Permutationen

$$\rho = (1, 7, 5, 2, 3)(6, 4) = (1, 3)(1, 2)(1, 5)(1, 7)(6, 4)$$

är udda.

Sats 7.2 Mängden av alla jämna permutationer bildar en grupp m a p sammansättningen och kallas för den alternerade gruppen för n element. Betecknas A_n.

Definition. En grupp $(G, *)$ kallas abelsk om

$$a * b = b * a \text{ då } a, b \in G$$

Sats 6.3. S_n är inte abelsk då $n \geq 3$.

DELGRUPPER

En **delgrupp** till en grupp G är en delmängd $H \subseteq G$ så att H bildar en grupp under samma operation som G. Om $H \neq G$ är H en äkta delgrupp. Om $H = \{e\}$ är H en trivial delgrupp.

Lemma. Låt G vara en grupp med operation $*$ och låt H vara en delgrupp till G. Då följande gäller:

(a) om f är det neutrala elementet i H och e är det neutrala elementet i G, så är $f = e$;

(b) om $a \in H$ så är inversen till a i H lika med inversen till a i G.

Bevis. (a) Eftersom f är det neutrala elementet i H, är $f*f = f$. Multiplicera likheten från höger med inversen f^{-1} till f i G. Tack vare associativiteten får vi

$$\begin{aligned} f^{-1} * (f * f) &= f^{-1} * f, \\ (f^{-1} * f) * f &= e, \\ e * f &= e, \\ f &= e. \end{aligned}$$

(b) Låt $a \in G$. Låt a^{-1} vara inversen till a i G och låt c vara inversen till a i H. Då är $a * c = c * a = f$ och därmed $a * c = c * a = e$, ty $e = f$ enligt (a). Detta innebär att c är inversen till a i G, dvs $c = a^{-1}$.

Sats 7.1. Låt G vara en grupp. En delmängd $H \subseteq G$ bildar en delgrupp om och endast om

(i) H är icke-tom;

(ii) $a * b \in H$ för alla $a, b \in H$;

(iii) $a^{-1} \in H$ för alla $a \in H$.

Bevis. $\Rightarrow$ Låt H vara en delgrupp till G. (i) gäller ty H har minst ett neutralt element; (ii) gäller, ty $*$ är en operation på H; (iii) gäller, ty om $a \in H$ så har a en invers a' i H och enligt lemma ovan a' är lika med inversen a^{-1} till a i G vilket ger $a^{-1} \in H$.

$\Leftarrow$ Låt H vara en delmängd till G som uppfyller (i), (ii) och (iii). (ii) betyder att $*$ är en operation på H. Associativiteten följer från att $*$ är associativ på hela G. Gruppens neutrala elementet e ligger i H eftersom om $a \in H$ (sådant element existerar enligt (i)) så är $a^{-1} \in H$ enligt (iii) och $e = a * a^{-1} \in H$ enligt (ii). Detta ger att e är ett neutralt element i H. Varje element $a \in H$ har en invers i H, nämligen a^{-1}, som ligger iH enligt (iii). Alltså är H en grupp m a p $*$.

Exempel 1. $U = \{z \in \mathbb{C} \mid |z| = 1\}$ är en delgrupp i $\mathbb{C} \setminus \{0\} = \mathbb{C}^*$ under multiplikation. (Visa!)

Exempel 2. Alla $(n \times n)$-matriser med reella element och med determinant lika med 1 är en delgrupp (betecknas $SL_n(\mathbb{R})$) till gruppen $GL_n(R)$ av alla $(n \times n)$-matriser med reella element och med determinant $\neq 0$ under matrismultiplikation. Vi har

$$A, B \in SL_n(\mathbb{R}) \Rightarrow \det A = 1 = \det B \Rightarrow \det(AB) = \det A \det B = 1 \Rightarrow AB \in SL_n(\mathbb{R})$$

vilket visar slutheten. Om $A \in SL_n(\mathbb{R})$ och A^{-1} är inversen till A så gäller $AA^{-1} = E$ (E är enhetsmatrisen), $1 = \det E =$

det $AA^{-1} = \det A \det A^{-1}$ vilket ger nu det $A^{-1} = 1$ så att $A^{-1} \in SL_n(\mathbb{R})$.

Exempel 3. De jämna permutationerna i S_n bildar en delgrupp - den **alternerande gruppen** (Sats 7.2).

Algebraiska strukturer, 28 januari

RELATIONER

En **relation** R på en mängd X är en godtycklig mängd bestående av par (x, y), där $x,\ y \in X$.

Man skriver $x \sim_R y$ ($x \sim y$) om $(x, y) \in R$. Men "$\sim$" ersätts oftast med andra tecken som traditionellt betecknar kända relationer t ex med "$\leq$" eller "$|$".

Exempel. 1. Låt $X = \mathbb{N}$ och låt $R_1 = \{(x, x), x \in \mathbb{N}\}$. R_1 beskriver likheten: $x \sim_{R_1} y$ omm $x = y$.

2. Låt $X = \mathbb{Z}$ och $R_2 = \{(x, x + 5k), x \in \mathbb{Z}, k \in \mathbb{Z}\}$. Då $x \sim_{R_2} y$ omm $5|(x - y)$.

3. Låt $X = \mathbb{R}$ och $R_3 = \{(x, y), x \leq y\}$. R_3 beskriver relationen "mindre eller lika".

EKVIVALENSRELATIONER

En relation $\sim$ på X är en **ekvivalensrelation** om

- $x \sim x$ för alla $x \in X$ (**reflexiv**)
- $x \sim y \Leftrightarrow y \sim x$ (**symmetrisk**)
- $x \sim y$ och $y \sim z \Rightarrow x \sim z$ (**transitiv**)

Relationerna R_1, R_2 är ekvivalensrelationer, R_3 är ej symmetrisk.

PARTITIONER

Låt X vara en mängd, $X_i \subseteq X$, $X_i \neq \emptyset$, $i \in I$. Man säger att X_i, $i \in I$, utgör en **partition** av X om

$$X = \cup_{i \in I} X_i \text{ och } X_i \cap X_j = \emptyset \text{ då } X_i \neq X_j.$$

Låt $\sim$ vara en ekvivalensrelation på X och $x \in X$. Mängden

$$[x] = \{y \in X, \text{ där } y \sim x\}, \quad x \in X.$$

$[x]$ kallas då för ekvivalensklassen till x under $\sim$.

Sats 9.1. Ekvivalensklasserna under varje ekvivalensrelation på X bildar en partition av X. Omvänt, givet en partition så finns det ekvivalensrelation på X, vars ekvivalensklasser utgörs precis av X_i, $i \in I$.

Bevis. 1. Låt $\sim$ vara en ekvivalensrelation på X. Eftersom $x \sim x$ för varje $x \in X$, gäller $x \in [x]$ och $X = \cup_{x \in X}[x]$ (unionen av alla ekvivalensklasserna).

Låt nu $[a]$ och $[b]$ vara två icke-disjunkta ekvivalensklasser. Vi vill visa att $[a] = [b]$. Då får vi att **två ekvivalensklasser antingen är lika eller disjunkta**. Eftersom $[a] \cap [b] \neq \emptyset$ finns det c som tillhör såväl $[a]$ som $[b]$. Ur symmetriet och transitiviteten följer att

$$c \in [a] \text{ och } c \in [b] \Rightarrow a \sim c \text{ och } c \sim b \Rightarrow a \sim b$$

Välj nu $x \in [a]$ godtyckligt. Då gäller $x \sim a$ som tillsammans med $a \sim b$ ger $x \sim b$ och därmed $x \in [b]$ och $[a] \subseteq [b]$. Av symmetriskäl har man också $[b] \subseteq [a]$ och alltså $[a] = [b]$.

2. Definiera $\sim$ enligt

$$x \sim y \Leftrightarrow \text{ } x \text{ och } y \text{ tillhör samma } X_i$$

Reflexivitet och symmetri är uppenbara. $\sim$ är transitiv, ty $x \sim y$ och $y \sim z \Leftrightarrow$ det finns $i \in I$ så att $x, y \in X_i$ och det finns $j \in I$ så att $y, z \in X_j$ varav $y \in X_i \cap X_j$. Eftersom $X_i \cap X_j \neq \emptyset$ omm $X_i = X_j$, får vi att $x, y, z \in X_i = X_j$, dvs $x \sim z$. Altså är $\sim$ en ekvivalensrelation. Det framgår också att ekvivalensklasser under $\sim$ utgörs av mängderna X_i, $i \in I$.

Ur sats 9.1 följer att två ekvivalensklasser antingen är lika eller disjunkta och dessutom $x \in [a]$ omm $[x] = [a]$.

DELBARHET

Definition. Om a och b är två heltal så säger man att b **delar** a om $a = bq$, där q är ett heltal. Detta betecknas $b|a$.

Några egenskaper hos delbarhetsrelation.

Låt a, b, $c \in \mathbb{Z}$. Då gäller

(a) om $d|a$ och $d|b$ så gäller $d|(a \pm b)$;

(b) om $a|b$ och $b|c$ så gäller $a|c$;

(c) om $a|b$ och $b|a$ så är $b = \pm a$.

KONGRUENSER

Låt n vara ett positivt heltal, a, $b \in \mathbb{Z}$. Man säger att a och b är **kongruenta modulo** n om $n|(a-b)$. Man skriver $a \equiv b \mod n$ eller $a \equiv_n b$. Uttrycket $a \equiv b \mod n$ kallas **kongruens**.

Sats 10.1. Kongruens modulo n är en ekvivalensrelation på $\mathbb{Z}$ för varje positivt heltal n.

Bevis. Reflexiv: $a \in \mathbb{Z} \Rightarrow a \equiv a \mod n$, ty $a - a = 0$ och $n|0$.

Symmetrisk: $a, b \in \mathbb{Z}$ och $a \equiv b \mod n \Rightarrow n|(a-b) \Rightarrow n|(b-a) \Rightarrow b \equiv a \mod n$.

Transitiv: $a, b, c \in \mathbb{Z}$, $a \equiv b \mod n$, $b \equiv c \mod n \Rightarrow n|(a-b)$ och $n|(b-c) \Rightarrow n|((a-b)+(b-c))$, dvs $n|(a-c) \Rightarrow a \equiv c \mod n$.

Ekvivalensklasserna under denna ekvivalensrelation kallas kongruensklasserna modulo n.

Exempel. Det finns tre kongruensklasser modulo 3:

$[0] = \{x \in \mathbb{Z}, x \equiv_3 0\} = \{x \in \mathbb{Z}, 3|x\} = \{\ldots, -3, 0, 3, \ldots\}$,

$[1] = \{x \in \mathbb{Z}, x \equiv_3 1\} = \{x \in \mathbb{Z}, 3|(x-1)\} = \{\ldots, -2, 1, 4, \ldots\}$,

$[2] = \{x \in \mathbb{Z}, x \equiv_3 2\} = \{x \in \mathbb{Z}, 3|(x-2)\} = \{\ldots, -1, 2, 5, \ldots\}$.

Divisionsalgoritmen. Om a och b är heltal och $b \neq 0$ så är

$$a = bq + r, \text{ där } 0 \leq r < |b|.$$

Både q och r är definierade entydigt av a och b.

Definition. Talen q och r i Divisionsalgoritmen kallas för **kvoten** och respektive **resten** vid division av a med b.

Sats 10.2. Låt n vara ett positivt heltal. Varje heltal är kongruent modulo n med precis ett av heltalen $0, 1, \ldots, n-1$.

Bevis. Låt $a \in \mathbb{Z}$. Enligt Divisionsalgoritmen är

$$a = nq + r, \text{ där } 0 \leq r < n.$$

Då är $a - r = nq$ vilket medför att $n|(a-r)$ och $a \equiv_n r$. Vi har alltså att a är kongruent med minst ett av heltalen $0, 1, \ldots, n-1$. För att visa unikness antar vi att $a \equiv_n s$, där $0 \leq s < n$. Då gäller $a - s = nt$, för något heltal t, och $a = nt + s$. Detta medför att $s = r$, ty resten är definierad entydigt av a och n.

För kongruensrelationen modulo n har man

$$[x] = [r], \text{ där } r \text{ är resten vid divisionen av } x \text{ med } n \ ,$$

ty $x \equiv_n r$ och därmed $x \in [r]$, och eftersom olika kongruensklasser saknar gemensamma element får vi $[x] = [r]$.

Av sats 10.2 följer att det finns precis n kongruensklasser modulo n: $[0], [1], \ldots, [n-1]$.

Mängden av alla kongruensklasser kommer att betecknas med $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ eller $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ eller enkelt $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

Definition. För $[a], [b] \in \mathbb{Z}_n$ definierar vi

$$[a] \oplus [b] = [a + b] \text{ och } [a] \odot [b] = [ab].$$

Är operationerna väl-definierade?

Lemma. I $\mathbb{Z}_n$ gäller följande:

om $[a_1] = [a_2]$ och $[b_1] = [b_2]$ så är $[a_1 + b_1] = [a_2 + b_2]$ och $[a_1 b_1] = [a_2 b_2]$.

Sats 11.1. $\mathbb{Z}_n$ är en abelsk grupp med avseende på operationen $\oplus$.

Bevis. Associativitet:

$$[a] \oplus ([b] \oplus [c]) = [a] \oplus [b + c] = [a + (b + c)]$$
$$([a] \oplus [b]) \oplus [c] = [a + b] \oplus [c] = [(a + b) + c]$$

så att $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$, ty $a + (b + c) = (a + b) + c$.

$[0]$ är det neutrala elementet. Inversen till $[r]$ är $[-r]$, ty $[r] \oplus [-r] = [r - r] = [0] = [-r + r] = [-r] \oplus [r]$.

Alltså är $\mathbb{Z}_n$ en grupp. Den är abelsk, ty $[a] \oplus [b] = [a + b] = [b + a] = [b] \oplus [a]$.

Obs! $(\mathbb{Z}_n, \odot)$ är aldrig en grupp, ty $[0]$ saknar invers. $\mathbb{Z}_n \setminus \{[0]\}, \odot)$ behöver inte heller vara en grupp, ty t ex $[2] \odot [3] = [6] = [0]$ i $\mathbb{Z}_6$.

Algebraiska strukturer, 30 januari

Låt a och b vara heltal. Med **största gemensamma delaren** till a och b ($a \neq 0$ eller $b \neq 0$) menar man ett positivt heltal d så att

1) $d|a$ och $d|b$;

2) d är delbart med varje gemensam delare till a och b.

Betecknas $SGD(a,b)$ eller (a,b). $SGD(0,0) = 0$.

$SGD(a,b)$ är definierad entydigt, ty om både d och d' uppfyller villkoren ovan så gäller $d|d'$ och $d'|d$ vilket innebär att $d = \pm d'$.

Om $SGD(a,b) = 1$ så säger man att a och b är **relativt prima**.

$SGD(a,b)$ kan beräknas med hjälp av **Euklides algoritm**: Man bildar en divisionkedja

$$
\begin{aligned}
&a = bq_1 + r_1, \quad 0 \leq r_1 < |b|,\\
&b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1,\\
&r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2,\\
&\ldots\\
&r_{n-2} = r_{n-1} q_n + r_n, \quad 0 \leq r_n < r_{n-1},\\
&r_{n-1} = r_n q_{n+1}.
\end{aligned}
$$

Vi påstår att $r_n = SGD(a,b)$. $r_n|a$ och $r_n|b$, ty från likheterna följer att $r_n|r_{n-1} \Rightarrow r_n|r_{n-2} \Rightarrow \ldots r_n|b \Rightarrow r_n|a$.

Om g nu är en godtycklig gemensam delare till a och b så visar den första likheten att $g|r_1$. Alltså ger den andra att $g|r_2$, osv, $g|r_n$. Detta visar påståendet.

Proposition. För varje par av heltal a och b finns det två heltal m och n sådana att $SGD(a,b) = am + bn$.

m och n kan beräknas med hjälp av Euklides algoritm.

Med **minsta gemensamma multipeln** till a och b menar man ett positivt heltal m som är delbart med a och b och som delar varje gemensam multipeln av a och b. Minsta gemensamma multipeln av a och b definieras entydigt av dessa tal (varför?). Betecknas $MGM(a,b)$.

Man säger att ett positivt heltal p är ett **primtal** om p har exakt två olika positiva delare: 1 och p.

Aritmetikens fundamentalsats. Varje heltal $n > 1$ är en entydig produkt av primtal dvs om

$$n = p_1 p_2 \ldots p_m = p'_1 p'_2 \ldots p'_n,$$

där p_i och p'_j är primtal så är $m = n$ och vid lämplig numrering av faktorerna är $p_i = p'_i$.

Lemma 1. Låt p vara ett primtal, $a, b \in \mathbb{Z}$. Om $p|ab$ så gäller $p|a$ eller $p|b$.

Bevis av Lemma 1. Antag att $p \not| a$. Då är $SGD(p,a) = 1$ och det finns m, $n \in \mathbb{Z}$ så att $1 = pm + an$. Detta ger $b = pbm + abn$. Eftersom $p|pbm$ och $p|abn$, får vi $p|b$.

Lemma 2. Låt p vara ett primtal $a_1, \ldots, a_k \in \mathbb{Z}$. Om $p|a_1 \ldots a_k$ så gäller $p|a_i$ för något i.

Bevis av Lemma 2. Vi visar påståendet med induktion med avseende på antalet faktorer k i produkten. Fallet $k = 1$ är klart. Låt $k > 1$ och antag att $p|a_1 \dots a_{k-1}$ medför $p|a_i$ för något $i \in \{1, \dots, k-1\}$. Låt $p|a_1 \dots a_k$. Enligt Lemma 1, $p|a_k$ eller $p|a_1 \dots a_{k-1}$. Om $p|a_k$ så] är vi klara. I annat fall ger induktionsantagandet att $p|a_i$ för något $i \in \{1, \dots, k-1\}$. Beviset är klart.

Bevis av satsen. Först visar vi med induktion att varje heltal $n > 1$ är en produkt av primtal. $n = 2$ är klart. Låt $n > 2$ och antag att varje heltal k, $1 < k < n$, är en produkt av primtal. Låt p vara minsta äkta delaren till n ($p \neq 1$). Då är p ett primtal, ty annars har p en äkta delare som är automatiskt en delare till n. Vi har $n = pq$, där $1 \leq q < n$. Enligt antagandet är q en produkt av primtal vilket visar att n är en sådan produkt.

Entydigheten. Låt

$$p_1 p_2 \dots p_m = p'_1 p'_2 \dots p'_n, \tag{1}$$

där p_i och p'_j är primtal. Primtalet p_1 delar $p_1 \dots p_m$. Detta ger $p_1 | p'_1 p'_2 \dots p'_n$. Enligt Lemma 2 $p_1 | p'_k$ för något k och därmed $p_1 = p'_k$. Vi eliminerar p_1 från vänster och p'_k från höger i likheten (1) och får

$$p_2 \dots p_m = p'_1 \dots p'_{k-1} p'_{k+1} \dots p'_n.$$

Vi upprepar samma argumenter och får $m = n$, varje p_i är lika med något p'_j, ty vi inte kan ha alla primtal borttagna på en av sidorna och ha några kvar på den andra.

Algebraiska strukturer, 4 februari

GRUPPER

Några enkla egenskapper hos grupper. Låt G vara en grupp. Då gäller följande

- $a, b, c \in G$ och $ab = ac \Rightarrow b = c$;
- $a, b, c \in G$ och $ba = ca \Rightarrow b = c$;
- $a, b \in G \Rightarrow$ ekvationen $ax = b$ ($xa = b$) har precis en lösning $x = a^{-1}b$ (respektive $x = ba^{-1}$);
- $a \in G \Rightarrow (a^{-1})^{-1} = a$;
- $a, b \in G \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$

Bevis=Övning.

Antalet element i en ändlig grupp kallas **gruppens ordning** och betecknas $o(G)$ eller $|G|$. Om G har oändligt många element säger vi att G har oändlig ordning och skriver $o(G) = \infty$ eller $|G| = \infty$.

CYKLISKA GRUPPER

Låt G vara en grupp, $a \in G$. Vi vill bestämma den minsta delgrupp till G som innehåller a. Den måste innehålla

$$a, aa = a^2, aaa = a^3, \ldots, \underbrace{aa \ldots a}_{n \text{ gånger}} = a^n,$$

identitetselementet $e = a^0$

$$a^{-1}, (aa)^{-1} = a^{-1}a^{-1} = a^{-2}, \ldots \underbrace{(aa \ldots a)}_{n \text{ ggr}}{}^{-1} = \underbrace{a^{-1}a^{-1} \ldots a^{-1}}_{n \text{ ggr}} = a^{-n}.$$

Det är lätt att visa att $a^n a^m = a^{n+m}$ och $(a^n)^{-1} = a^{-n}$ för varje $m, n \in \mathbb{Z}$. Enligt Sats 7.1 mängden $\{a^n, n \in \mathbb{Z}\}$ är en delgrupp till G ($a^n a^m = a^{n+m} \in \{a^n, n \in \mathbb{Z}\}$, $(a^n)^{-1} = a^{-n} \in \{a^n, n \in \mathbb{Z}\}$). Denna delgrupp kallas för **delgruppen genererad av** a och betecknas med $\langle a \rangle$. Med den additiva notationen måste man ersätta a^n med $na (= \underbrace{a + a + \ldots + a}_{n \text{ ggr}}$ då $n > 0$ och $\underbrace{(-a) + (-a) \ldots + (-a)}_{n \text{ ggr}}$ då $n < 0$).

Om H är en grupp och $H = \langle a \rangle$ för något element $a \in H$ så kallas H för en **cyklisk grupp**.

Exempel 1. Låt $G = \{-1, 1\}$ med den vanliga multiplikationen som operation. Då är $G = \langle -1 \rangle = \{(-1)^n, n \in \mathbb{Z}\} \neq \langle 1 \rangle$.

2. Låt $G = \mathbb{C} \setminus \{0\}$, $a = i$. Vi får

$$i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1, i^5 = i, i^6 = -1, \ldots$$

så att vi endast får fyra olika tal. Å andra sidan är $i^{-1} = i^3$ så att varje negativ potens är lika med en positiv. Vi får $\langle i \rangle = \{1, i, -1, -i\}$.

3. Låt $G = \mathbb{Z}$ med additionen som operation. Då är $\mathbb{Z} = \{n \cdot 1, n \in \mathbb{Z}\} = \langle 1 \rangle$. $\mathbb{Z}$ är oändlig.

Det finns två möjligheter för potenser a^n i G:

- $a^n \neq a^m$ för alla $n \neq m$ (i detta fall är $\langle a \rangle$ oändlig).
- det finns $r < s$ så att $a^r = a^s$ (enligt sats 14.3 är $\langle a \rangle$ ändlig).

Sats 14.3. Låt G vara en grupp, $a \in G$. Antag att det finns $r < s$, $r, s \in \mathbb{Z}$ så att $a^r = a^s$. Då gäller följande:

- (i) Det finns ett minsta positiva heltal n så att $a^n = e$.
- (ii) Om $t \in \mathbb{Z}$ så gäller $a^t = e$ om och endast om $n|t$.
- (iii) Elementen $e = a^0, a, \ldots, a^{n-1}$ är olika och

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Bevis. (i) $a^r = a^s, r < s \Leftrightarrow a^{s-r} = e, s - r > 0$. Detta visar att det finns ett positivt heltal $n \in \mathbb{Z}$ så att $a^n = e$. Eftersom mängden av de positiva heltalen är nedåt begränsad finns det minsta positiva heltal som uppfyller $a^n = e$.

(ii) Låt $a^t = e$, $t > 0$. Då är $t \geq n$. Divisionen av t med n ger $t = nq + r$, där $0 \leq r < n$. Vi får då

$$e = a^t = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = a^r,$$

som medför att $r = 0$, dvs $t = nq$ och $n|t$.

Om n delar t så är $t = nq$ och $a^t = (a^n)^q = e$.

(iii) Låt $r < s \leq n$. Antag att $a^r = a^s$. Då är $a^{s-r} = e$ och $0 < s - r < n$ vilket är omöjligt, ty n är det minsta positiva heltal så att $a^n = e$. Detta visar att $e, a, \ldots, a^{n-1}$ är olika.

Vidare, varje a^N är lika med en av potenserna $a^0, a^1, \ldots, a^{n-1}$, ty $N = qn + r$, $0 \leq r < n$ och $a^N = a^{qn+r} = a^r$. Detta betyder att $\langle a \rangle = \{e, a, \ldots a^{n-1}\}$.

Det minsta positiva heltal n så att $a^n = e$ (additivt: $na = e$) kallas för **ordningen** av a och betecknas $o(a)$. Om sådant n inte existerar skriver vi $o(a) = \infty$. Enligt sats 14.3 är

$$o(a) = |\langle a \rangle|$$

Exempel 1. $G = (\mathbb{C} \setminus \{0\}, \cdot)$. Då är $o(i) = 4$ (se exemplet ovan).

2. $G = (\mathbb{Z}_6, \oplus)$. $2[3] = [3] \oplus [3] = [6] = [0]$, dvs $o([3]) = 2$. $2[2] = [4] \neq [0]$, $3[2] = [6] = [0]$ och $o([2]) = 3$.

SIDOKLASSER

Låt $G = \mathbb{Z}$ (med addition). Kongruensen modulo n är en ekvivalensrelation på $\mathbb{Z}$ vars ekvivalensklasserna (kongruensklasserna) är $[0], [1], \ldots, [n-1]$ där

$[r] =$ alla heltal som lämnar resten r vid division med n,

dvs

$$[0] = \{kn, k \in \mathbb{Z}\}$$
$$[1] = \{kn + 1, k \in \mathbb{Z}\}$$
$$\ldots$$
$$[r] = \{kn + r, k \in \mathbb{Z}\}$$
$$\ldots$$
$$[n-1] = \{kn + (n-1), k \in \mathbb{Z}\}$$

Vi har $\mathbb{Z} = [0] \cup [1] \cup \ldots \cup [n-1]$. Dessutom är mängden $[0]$ en delgrupp till G och $[r] = [0] + r = \{a + r, a \in [0]\}$. $[0] + r$ kallas en högersidoklass till delgruppen $[0]$. Vi fick en uppdelning av $\mathbb{Z}$ i parvis disjunkta sidoklasser:

$$\mathbb{Z} = [0] \cup [0] + 1 \cup \ldots \cup [0] + (n-1)$$

Mängden $Hg = \{hg, h \in H\}$ (additivt: $H + g = \{h + g, h \in H\}$), där g är ett fixt element i G och H är en delgrupp till G kallas en **högersidoklass** till H i G. Man säger att g är en representant för Hg.

Vi har $a \equiv b \mod n$ omm $a - b \in [0]$, dvs $n|a-b$ och kongruensen modulo n definierar en ekvivalensrelation.

Sats 16.1. Låt H vara en delgrupp till en grupp G. Då är relationen $\sim$ på G definierade enligt

$$a \sim b \text{ omm } ab^{-1} \in H \text{ (additivt: } a - b \in H)$$

en ekvivalensrelation på G med ekvivalensklasserna Hg, $g \in G$ (additivt: $H + g$).

Bevis. Reflexiv: $x \sim x$ ty $xx^{-1} = e \in H$.

Symmetrisk: $x \sim y \Leftrightarrow xy^{-1} \in H \Leftrightarrow (xy^{-1})^{-1} \in H$. Eftersom $(xy^{-1})^{-1} = (y^{-1})^{-1}x^{-1} = yx^{-1}$ får vi $yx^{-1} \in H$ och därmed $y \sim x$.

Transitiv: $x \sim y$ och$y \sim z \Rightarrow xy^{-1} \in H$ och $yz^{-1} \in H$. Eftersom H är en delgrupp får vi att $xz^{-1} = (xy^{-1})(yz^{-1}) \in H$ dvs $x \sim z$.

Altså är $\sim$ en ekvivalensrelation.

Ekvivalensklassen till $x \in G$ är

$$[x] = \{y \in G, y \sim x\} = \{y, yx^{-1} \in H\} = \{y, y \in Hx\} = Hx.$$

Enligt Sats.9.1. och Sats.16.1 får vi att högersidoklasserna bildar en partition av G dvs

- $G = \cup_{g \in G} Hg$,
- $Hg_1 \cap Hg_2 \neq \emptyset \Rightarrow Hg_1 = Hg_2$, dvs två högersidoklasser antingen är lika eller disjunkta.

Dessutom har vi att

- $g \in Hg$
- $g' \in Hg \Leftrightarrow Hg = Hg'$,
- $g' \in Hg \Leftrightarrow g'g^{-1} \in H$.

Exempel. Låt $G = \mathbb{R}^2$ vara gruppen av alla vektorer i planet med avseende på addition av vektorer. Låt H vara den delgrupp till G som består av alla vektorer på x-axeln. Om $\mathbf{v}$ är en vektor så består sidoklassen $H + \mathbf{v}$ av alla vektorer som man får genom att addera $\mathbf{v}$ till alla vektorer på x-axeln. Då får man alla vektorer som slutar på den linje som är parallell med x-axeln och som går igenom ändpunkten av $\mathbf{v}$. Olika sådana linjer svarar mot olika sidoklasser.

Man kan definiera **vänstersidoklasser** på samma sätt:

$$gH = \{gh, h \in H\}.$$

Om gruppen är abelsk har vi att $gH = Hg$. Alla egenskaper hos högersidoklasser visas analogt för vänstersidoklasser. Om gruppen inte är abelsk vänster- och högersidoklasser kan vara olika.

Algebraiska strukturer, 6 februari

SIDOKLASSER

Låt $G = \mathbb{Z}$ (med addition). Kongruensen modulo n är en ekvivalensrelation på $\mathbb{Z}$ vars ekvivalensklasserna (kongruensklasserna) är $[0], [1], \ldots, [n-1]$ där

$[r] =$ alla heltal som lämnar resten r vid division med n,

dvs

$$[0] = \{kn, k \in \mathbb{Z}\}$$
$$[1] = \{kn + 1, k \in \mathbb{Z}\}$$
$$\ldots$$
$$[r] = \{kn + r, k \in \mathbb{Z}\}$$
$$\ldots$$
$$[n-1] = \{kn + (n-1), k \in \mathbb{Z}\}$$

Vi har $\mathbb{Z} = [0] \cup [1] \cup \ldots \cup [n-1]$. Dessutom är mängden $[0]$ en delgrupp till G och $[r] = [0] + r = \{a + r, a \in [0]\}$. $[0] + r$ kallas en högersidoklass till delgruppen $[0]$. Vi fick en uppdelning av $\mathbb{Z}$ i parvis disjunkta sidoklasser:

$$\mathbb{Z} = [0] \cup [0] + 1 \cup \ldots \cup [0] + (n-1)$$

Mängden $Hg = \{hg, h \in H\}$ (additivt: $H + g = \{h + g, h \in H\}$), där g är ett fixt element i G och H är en delgrupp till G kallas en **högersidoklass** till H i G. Man säger att g är en representant för Hg.

Vi har $a \equiv b \mod n$ omm $a - b \in [0]$, dvs $n|a - b$ och kongruensen modulo n definierar en ekvivalensrelation.

Sats 16.1. Låt H vara en delgrupp till en grupp G. Då är relationen $\sim$ på G definierade enligt

$$a \sim b \text{ omm } ab^{-1} \in H \text{ (additivt: } a - b \in H)$$

en ekvivalensrelation på G med ekvivalensklasserna Hg, $g \in G$ (additivt: $H + g$).

Bevis. Reflexiv: $x \sim x$ ty $xx^{-1} = e \in H$.

Symmetrisk: $x \sim y \Leftrightarrow xy^{-1} \in H \Leftrightarrow (xy^{-1})^{-1} \in H$. Eftersom $(xy^{-1})^{-1} = (y^{-1})^{-1}x^{-1} = yx^{-1}$ får vi $yx^{-1} \in H$ och därmed $y \sim x$.

Transitiv: $x \sim y$ och$y \sim z \Rightarrow xy^{-1} \in H$ och $yz^{-1} \in H$. Eftersom H är en delgrupp får vi att $xz^{-1} = (xy^{-1})(yz^{-1}) \in H$ dvs $x \sim z$.

Altså är $\sim$ en ekvivalensrelation.

Ekvivalensklassen till $x \in G$ är

$$[x] = \{y \in G, y \sim x\} = \{y, yx^{-1} \in H\} = \{y, y \in Hx\} = Hx.$$

Enligt Sats.9.1. och Sats.16.1 får vi att högersidoklasserna bildar en partition av G dvs

- $G = \cup_{g \in G} Hg$,
- $Hg_1 \cap Hg_2 \neq \emptyset \Rightarrow Hg_1 = Hg_2$, dvs två högersidoklasser antingen är lika eller disjunkta.

Dessutom har vi att

- $g \in Hg$
- $g' \in Hg \Leftrightarrow Hg = Hg'$,
- $g' \in Hg \Leftrightarrow g'g^{-1} \in H$.

Exempel. Låt $G = \mathbb{R}^2$ vara gruppen av alla vektorer i planet med avseende på addition av vektorer. Låt H vara den delgrupp till G som består av alla vektorer på x-axeln. Om $\mathbf{v}$ är en vektor så består sidoklassen $H + \mathbf{v}$ av alla vektorer som man får genom att addera $\mathbf{v}$ till alla vektorer på x-axeln. Då får man alla vektorer som slutar på den linje som är parallell med x-axeln och som går igenom ändpunkten av $\mathbf{v}$. Olika sådana linjer svarar mot olika sidoklasser.

Man kan definiera **vänstersidoklasser** på samma sätt:

$$gH = \{gh, h \in H\}.$$

Om gruppen är abelsk har vi att $gH = Hg$. Alla egenskaper hos högersidoklasser visas analogt för vänstersidoklasser. Om gruppen inte är abelsk vänster- och högersidoklasser kan vara olika.

Proposition. Låt H vara en ändlig delgrupp till en grupp G. Då är $|Hg| = |H|$ för varje $g \in G$.

Bevis. Låt $H = \{h_1, \ldots, h_n\}$. Då är $Hg = \{hg_1, \ldots, hg_n\}$. Produkterna $h_i g$ är olika ty $h_i g = h_j g$ ger $h_i = h_j$. Detta visar att antalet element i H är lika med antalet element i Hg.

Lagranges sats. Låt H vara en delgrupp till en ändlig grupp. Då är $o(H)|o(G)$.

Bevis. Högersidoklasserna Hg bildar en partition av G, dvs $G = Hg_1 \cup Hg_2 \cup \ldots \cup Hg_n$ och $Hg_i \cap Hg_j = \emptyset$. Då är

$$o(G) = |Hg_1| + |Hg_2| + \ldots + |Hg_n| =$$
$$(\text{ enligt propositionen ovan }) = |H| + |H| + \ldots + |H| = n|H|$$

vilket ger nu att $|H| (= o(H))$ delar $o(G)$.

INDEX

Beviset av Lagranges sats visar att antalet högersidoklasser är lika med $o(G) : o(H)$. När man bevisar Lagranges sats med hälp av vänstersidoklasser i stället för högersidoklasser får man att $o(G) : o(H)$ är lika med antalet vänstersidoklasser.

Antalet högersidoklasser (eller vänstersidoklasser) till H i G kallas för **index** av H i G. Indexet betecknas ofta med $[G : H]$.

Följdsatser.

- **1.** Låt G vara en ändlig grupp, $a \in G$. Då $o(a)|o(G)$.

- **2.** Om $o(G) = p$, där p är ett primtal, så saknar G äkta delgrupper H dvs $H \neq \{e\}, G$.
- **3.** Varje grupp av primtalsordning är cyklisk.
- **4.** Om $o(G) = N$ och $a \in G$ så är $a^N = e$.

Bevis. 1. Om $a \in G$ så ordningen $o(a)$ av a lika med ordningen av delgruppen $\langle a \rangle$ genererad av a. Enligt Lagranges sats är alltså $o(a)$ en delare till $o(G)$.

2. Följer direkt från Lagranges sats ty varje primtal p saknar delare $\neq 1, p$.

3. Om $a \in G$, $a \neq e$ så är $\langle a \rangle$ en delgrupp till G och $\langle a \rangle \neq \{e\}$. Enligt **2** är $\langle a \rangle = G$.

4. Om $a \in G$ så är $o(a)|N$ enligt **1** och $N = no(a)$ för något heltal n. Vidare, $a^N = a^{no(a)} = (a^{o(a)})^n = e^n = e$.

Exempel. Med häjlp av Lagranges sats skall vi beskriva delgrupper till S_3.

$o(S_3) = 3! = 6$ och $S_3 = \{(1), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$.

Enligt Lagranges sats är de eventuella ordningarna av delgrupper till S_3 lika med 1, 2, 3, 6.

Det är klart att $o(H) = 1$ ger $H = \{(1)\}$ och $o(H) = 6$ ger $H = S_3$.

Om $o(H) = 2$ så måste $H = \{(1), g\}$ där g har ordning 2. Det finns 3 sådana : $(1,2)$, $(1,3)$, $(2,3)$. Alltså har vi tre delgrupper av ordning 2: $\{(1), (1,2)\}$, $\{(1), (1,3)\}$, $\{(1), (2,3)\}$.

Om $o(H) = 3$ så är $H = \{(1), g, g^2\}$ där $o(g) = 3$. Det finns 2 sådana element: $(1,2,3)$ och $(1,3,2)$. Eftersom $(1,2,3)(1,2,3) = (1,3,2)$, genererar de samma delgruppen $\{(1), (1,2,3), (1,3,2)\}$.

Varning. I allmänhet är det inte sant att om d är en delare till $o(G)$ så har G en delgrupp av ordning d. Men det gäller för cykliska grupper.

Sats. Låt G vara en ändlig cyklisk grupp av ordning n: $G = \langle a \rangle = \{e, a, \ldots . a^2\}$. Då gäller följande:

- Varje delgrupp till G är cyklisk
- Om $1 \leq k < n$ så genererar a^k en delgrupp av ordning $n/SGD(n,k)$.
- För varje positiv delare d till n har G precis en delgrupp av ordning d. Den är $\langle a^{n/d} \rangle$.

Exempel. Vilka delgrupper har $\mathbb{Z}_{16}$?

Enligt satsen ovan varje delgrupp av $\mathbb{Z}_{16}$ är cyklisk och för varje delare d till 16 finns det precis en delgrupp av ordning d.

Positiva delarna till 16: 1, 2, 4, 8, 16. Det finns 5 delgrupper:
$H_1 = \langle [0] \rangle$,
$H_2 = \langle \frac{16}{2}[1] \rangle = \{[0], [8]\}$,
$H_3 = \langle \frac{16}{4}[1] \rangle = \{[0], [4], [8], [12]\}$,
$H_4 = \langle \frac{16}{8}[1] \rangle = \{[0], [2], [4], [6], [8], [10], [12], [14]\}$,
$H_5 = \langle \frac{16}{16}[1] \rangle = \mathbb{Z}_{16}$.

ISOMORFIER

Exempel. Låt $G_1 = \mathbf{Z}_2 = \{[0],[1]\}$ med $\oplus$ och $G_2 = S_2 = \{(1),(1,2)\}$ med sammansätningen $\circ$. Grupptabellerna för G_1 och G_2 är följande

$\oplus$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\circ$	(1)	$(1,2)$
(1)	(1)	$(1,2)$
$(1,2)$	$(1,2)$	(1)

Observera att om vi skriver (1) istället för $[0]$ och $(1,2)$ istället för $[1]$ i första tabellen får vi den andra. Grupperna G_1 och G_2 är "lika" och det är bara deras element som betecknas på olika sätt. Betrakta avbildningen $\theta : \mathbf{Z}_2 \mapsto S_2$: $\theta([0]) = (1)$, $\theta([1]) = (1,2)$. Vi får att θ är en bijektion och

$$\theta([x] \oplus [y]) = \theta([x]) \circ \theta([y])$$

för godtyckliga $[x]$, $[y] \in \mathbf{Z}_2$.

Två grupper, G och H, är **isomorfa** om det finns en bijektion $\theta : G \mapsto H$, sådan att

$$\theta(a * b) = \theta(a) \# \theta(b), \text{ för alla } a, b \in G,$$

där $*$ är operationen i G och $\#$ är operationen i H.

Avbildningen θ kallas då en **isomorfi**, och vi skriver $G \approx H$.

Grupperna G_1 och G_2 från exemplet ovan är alltså isomorfa.

Exempel. Betrakta följande grupper: $(\mathbf{Z}, +)$ och $(2\mathbf{Z}, +)$. Definiera $\theta : \mathbf{Z} \mapsto 2\mathbf{Z}$ enligt $\theta(n) = 2n$ för varje $n \in \mathbf{Z}$. Klart att θ är bijektiv och $\theta(n+m) = 2(n+m) = 2n + 2m = \theta(n) + \theta(m)$ gäller för alla heltal m och n, dvs θ bevarar addition. Detta visar att θ är en isomorfi och $\mathbf{Z} \approx 2\mathbf{Z}$, fast $2\mathbf{Z} \subset \mathbf{Z}$.

Sats 18.1. Låt G vara en grupp med operation $*$, låt H vara en grupp med operation $\#$, och låt $\theta : G \mapsto H$ vara en avbildning sådan att $\theta(a * b) = \theta(a) \# \theta(b)$ för alla a, $b \in G$. Då

- **1.** $\theta(e_G) = e_H$
- **2.** $\theta(a^{-1}) = \theta(a)^{-1}$ för varje $a \in G$
- **3.** $\theta(a^k) = \theta(a)^k$ för varje $a \in G$
- **4.** $\theta(G)$, bilden av θ, är en delgrupp till H.
- **5.** Om θ är en-entydig så är $G \approx \theta(G)$

Satsen skall visas senare.

Sats 19.1. Antag att G och H är grupper och $G \approx H$. Då gäller

- $|G| = |H|$.
- G är abelsk $\Rightarrow$ H är abelsk.

- G är cyklisk $\Rightarrow$ H är cyklisk.
- G har en delgrupp av ordning n $\Rightarrow$ H har en delgrupp av ordning n.
- G har ett element av ordning n $\Rightarrow$ H har ett element av ordning n.

Exempel. 1. $\mathbf{Z}_5$ och $\mathbf{Z}_6$ är inte isomorfa, ty $|\mathbf{Z}_5| = 5$ men $|\mathbf{Z}_6| = 6$.

2. $\mathbf{Z}_2 \times \mathbf{Z}_2$ och $\mathbf{Z}_4$ är inte isomorfa (**obs!** $|\mathbf{Z}_2 \times \mathbf{Z}_2| = |\mathbf{Z}_4| = 4$), ty varje element$\neq ([0],[0])$ i $\mathbf{Z}_2 \times \mathbf{Z}_2$ har ordning 2 (varför?), men $\mathbf{Z}_4$ har ett element av ordning 4, t ex $[1]$.

Sats 19.2. Varje cyklisk grupp av ordning n är isomorf med $\mathbf{Z}_n$. Dessutom, om G är en grupp av ordning p, där p är ett primtal, så är $G \approx \mathbf{Z}_p$.

Bevis. Om G är en cyklisk grupp av ordning n så finns det $a \in G$ sådant att $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. Vi definierar $\theta : G \mapsto \mathbf{Z}_n$ genom $\theta(a^k) = [k]$, $k \in \mathbf{Z}$. Definitionen av denna funktion beror inte på heltalet k som definierar potensen: om $a^{k_1} = a^{k_2}$ så är $[k_1] = [k_2]$ ty $a^{k_1 - k_2} = e$ implicerar att $n|(k_1 - k_2)$ och därmed $[k_1] = [k_2]$. Man kontrollerar lätt att olika element a^k, a^m har olika bilder: $[k] = [m]$ betyder att $n|(k-m)$ vilket ger $a^{k-m} = e$ och $a^k = a^m$. Funktionen θ är en-entydig. Klart att den är surjektiv. Detta visar att θ är en bijektion. Vi har också att

$$\theta(a^k * a^l) = \theta(a^{k+l}) = [k+l] = [k] \oplus [l] = \theta(a^k) \oplus \theta(a^l).$$

Alltså är θ en isomorfi.

Om G är en grupp av ordning p, där p är ett primtal så är G cyklisk enligt en av följdsatserna till Lagranges sats vilket ger nu att $G \approx \mathbf{Z}_p$.

Fundamentala satsen om ändliga abelska grupper. Varje ändlig grupp G är isomorf med en direkt produkt av cykliska grupper av typen $\mathbf{Z}_{p_1^{k_1}} \times \ldots \times \mathbf{Z}_{p_n^{k_n}}$, där p_i är primtal som kan vara lika. Direkta produkten är definierad entydigt av G om man bortser från faktorernas ordningsföljd.

Obs! Om G och H är grupper så är $G \times H \approx H \times G$

Exempel. Beskriv abelska grupper av ordning 100.

Vi har

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5 \cdot 5 = 2 \cdot 2 \cdot 5^2 = 2^2 \cdot 5^5.$$

Enligt satsen är varje abelsk grupp av ordning 100 isomorf med precis en av följande grupper:

$$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_5 \times \mathbf{Z}_5,\ \mathbf{Z}_{2^2} \times \mathbf{Z}_5 \times \mathbf{Z}_5,\ \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{5^5},\ \mathbf{Z}_{2^2} \times \mathbf{Z}_{5^5}.$$

Cayles sats. Varje ändlig grupp är isomorf med en permutations grupp.

Bevis. Multiplikationen till höger med ett element $a \in G$ ger en permutation, σ_a, av $G = \{a_1, a_2, \ldots, a_n\}$:

$$\sigma_a = \begin{pmatrix} a_1 & a_2 & \ldots a_n \\ a*a_1 & a*a_2 & \ldots a*a_n \end{pmatrix}$$

(Obs! alla $a*a_i$ är olika, ty $a*a_i = a*a_j$ ger $a_i = a_j$. Multiplikation med en produkt $a*b$ ger permutationen $\sigma_{a*b} = \sigma_a \circ \sigma_b$. Vi får alltså en avbildning $\theta : G \mapsto Sym(G)$: $\theta(a) = \sigma_a$ vilken uppfyller $\theta(a*b) = \theta(a) \circ \theta(b)$ för alla $a, b \in G$. Om $\theta(a) = \theta(b)$ så är $c*a = c*b$ för alla c, varav $a = b$. Låt H vara bilden av G. H är en delgrupp av $Sym(G)$ och $H \approx G$.

Följdsats. Varje grupp av ordning n är isomorf med en delgrupp av S_n.

Bevis. Man kan identifiera elementet a_i i G med talet i och ersätta $a*a_i = a_{p_i}$ med p_i för ett lämpligt index p_i. Då representerar vi σ_a med en permutation av talen $1, 2, \ldots, n$:

$$\sigma_a = \begin{pmatrix} 1 & 2 & \ldots n \\ p_1 & p_2 & \ldots p_n \end{pmatrix}$$

HOMOMORFIER

Låt $(G, *)$ och $(H, \#)$ vara två grupper. En avbildning $\theta : G \mapsto H$ mellan grupper kallas en **grupphomomorfi** eller bara homomorfi om

- $\theta(a * b) = \theta(a)\#\theta(b)$ för alla $a, b \in G$.

Exempel. 1. Betrakta $(\mathbb{Z}, +)$ och $(\mathbb{Z}_n, \oplus)$. Definiera $\theta : \mathbb{Z} \mapsto \mathbb{Z}_n$ genom $\theta(k) = [k]$, $k \in \mathbb{Z}$. Då är θ en homomorfi, ty $\theta(k+m) = [k+m] = [k] \oplus [m] = \theta(k) \oplus \theta(m)$. θ är inte bijektiv, ty $\theta(k) = \theta(k+n)$ för alla $k \in \mathbb{Z}$.

2. Absolutbellopet ger en grupphomomorfi från $(\mathbb{C} \setminus \{0\}, \cdot)$ till $(\mathbb{R} \setminus \{0\}, \cdot)$, ty om $\theta(z) = |z|$ så är $\theta(z_1 z_2) = |z_1 z_2| = |z_1||z_2| = \theta(z_1)\theta(z_2)$. θ är ej isomorfi (varför?).

3. Låt $G = G_1 \times G_2$ vara direkta produkten av grupper. Avbildningen $\pi_i : G \mapsto G_i$, där $\pi_i((g_1, g_2)) = g_i$ är en homomorfi. Varför?

Sats 18.2. Låt G vara en grupp med operation $*$, låt H vara en grupp med operation $\#$, och låt $\theta : G \mapsto H$ vara en homomorfi. Då gäller:

- **1.** $\theta(e_G) = e_H$.
- **2.** $\theta(a^{-1}) = \theta(a)^{-1}$ för varje $a \in G$.
- **3.** $\theta(a^k) = \theta(a)^k$ för varje $a \in G$.
- **4.** $\theta(G)$, bilden av θ, är en delgrupp till H.
- **5.** Om θ är en-entydig så är $G \approx \theta(G)$.

Bevis.

1. För a i G har vi att

$$\theta(a) = \theta(a * e_G) = \theta(a)\#\theta(e_G),$$

varför $\theta(e_G) = e_H$.

2. För alla a i G är

$$\theta(a)\#\theta(a^{-1}) = \theta(a * a^{-1}) = \theta(e_G) = e_H.$$

Alltså är $\theta(a)^{-1} = \theta(a^{-1})$.

3. Induktion med avseende på $k > 0$. Fallet $k = 1$ är klart. Antag att $\theta(a^k) = \theta(a)^k$. Då

$$\theta(a^{k+1}) = \theta(a^k * a) = \theta(a^k)\#\theta(a) = \theta(a)^k\#\theta(a) = \theta(a)^{k+1}.$$

Fallet $k < 0$ är en övning

4. Om $b = \theta(a)$ och $b' = \theta(a')$ i $\{\theta(g), g \in G\}$, så är

$$b\#b' = \theta(a)\#\theta(a') = \theta(a * a') \in \{\theta(g), g \in G\}$$

och

$$b^{-1} = \theta(a)^{-1} = \theta(a^{-1}) \in \{\theta(g), g \in G\}.$$

Alltså är bilden av θ en delgrupp till H.

5. Om θ är en-entydig så är $\theta : G \mapsto \theta(G)$ en bijektion, varav $G \approx \theta(G)$.

BILD OCH KÄRNA

Om $\theta : G \mapsto H$ är en grupphomomorfi ges bilden till θ av

$$Im\theta = \theta(G) = \{\theta(g), g \in G\}$$

och kärnan till θ av $\ker\theta = \{g \in G : \theta(g) = e_H\}$.

Sats 31.1. Låt $\theta : G \mapsto H$ vara en grupphomomorfi. Då är $\ker\theta$ en delgrupp till G. Dessutom, är θ injektiv omm $\ker\theta = \{e_G\}$.

Bevis. $e_G \in \ker\theta$, enligt Sats 18.2. a, $a' \in \ker\theta \Rightarrow a * a'$, $a^{-1} \in \ker\theta$, eftersom

$$\theta(a * a') = \theta(a)\#\theta(a') = e_H\#e_H = e_H$$

och

$$\theta(a^{-1}) = \theta(a)^{-1} = e_H^{-1} = e_H.$$

Detta visar att $\ker\theta$ är en delgrupp till G.

Antag att $\ker\theta = \{e_G\}$. För a, $b \in G$ gäler att

$$\theta(a) = \theta(b) \Leftrightarrow \theta(a)\#\theta(b)^{-1} = e_H \Leftrightarrow \theta(a * b^{-1}) = e_H \Leftrightarrow$$
$$\Leftrightarrow a * b^{-1} \in \ker\theta \Leftrightarrow a * b^{-1} = e_G \Leftrightarrow a = b.$$

Detta visar att θ avbildar olika element i G på olika element i H, dvs θ är injektiv.

Om θ är injektiv, så är $\theta(a) = e_H$ omm $a = e_G$, ty $\theta(a) = e_H = \theta(e_G)$.

NORMALA DELGRUPPER

En delgrupp N till en grupp G är **normal** om $gng^{-1} \in N$ för alla $n \in N$ och alla $g \in G$. Vi skriver $N \triangleleft G$.

Obs! I an abelsk grupp är alla delgrupper normala, ty $gng^{-1} = ngg^{-1} = n \in N$ för alla $g \in G$ och alla $n \in N$.

Övning. Visa att N är en normal delgrupp till en grupp G omm $gN = Ng$ för alla $g \in G$, dvs vänster- och högersidoklasser är lika.

Exempel. 1. Låt $G = S_3$, $N = \langle(1,2)\rangle = \{(1), (1,2)\}$ och $g = (2,3)$. Då är

$$Ng = \{(2,3), (1,2,3)\}, \qquad gN = \{(2,3), (1,3,2)\}$$

varav följer att N inte är normal.

2. Låt $G = GL_n(\mathbb{R})$ (alla $n \times n$-matriser med determinant $\neq 0$ med matrismultiplikation). Låt $N = SL_n(\mathbb{R})$ (alla $n \times n$-matriser vars determinant är 1).

Övning. Visa att N är en delgrupp till G.

N är normal, ty

$$\det(ABA^{-1}) = \det A \det B (\det A)^{-1} = \det B = 1$$

för varje $A \in G$ och $B \in N$.

Sats 21.2 (31.2). Om $\theta : G \mapsto H$ är en grupphomomorfi så är $\ker\theta$ en normal delgrupp till G.

Bevis. Om $g \in G$ och $n \in \ker\theta$ så har vi att

$$\theta(gng^{-1}) = \theta(g)\theta(n)\theta(g^{-1}) = \theta(g)e_H\theta(g)^{-1} = \theta(g)\theta(g)^{-1} = e_H$$

och därmed ligger gng^{-1} i $\ker\theta$.

Algebraiska strukturer, 18 februari

NORMALA DELGRUPPER

En delgrupp N till en grupp G är **normal** om $gng^{-1} \in N$ för alla $n \in N$ och alla $g \in G$. Vi skriver $N \triangleleft G$.

Obs! I an abelsk grupp är alla delgrupper normala, ty $gng^{-1} = ngg^{-1} = n \in N$ för alla $g \in G$ och alla $n \in N$.

Övning. Visa att N är en normal delgrupp till en grupp G omm $gN = Ng$ för alla $g \in G$, dvs vänster- och högersidoklasser är lika.

Exempel. 1. Låt $G = S_3$, $N = \langle (1,2) \rangle = \{(1), (1,2)\}$ och $g = (2,3)$. Då är

$$Ng = \{(2,3), (1,2,3)\}, \qquad gN = \{(2,3), (1,3,2)\}$$

varav följer att N inte är normal.

2. Låt $G = GL_n(\mathbb{R})$ (alla $n \times n$-matriser med determinant $\neq 0$ med matrismultiplikation). Låt $N = SL_n(\mathbb{R})$ (alla $n \times n$-matriser vars determinant är 1).

Övning. Visa att N är en delgrupp till G.

N är normal, ty

$$\det(ABA^{-1}) = \det A \det B (\det A)^{-1} = \det B = 1$$

för varje $A \in G$ och $B \in N$.

Sats 21.2 (31.2). Om $\theta : G \mapsto H$ är en grupphomomorfi så är $\ker \theta$ en normal delgrupp till G.

Bevis. $\ker \theta$ är en delgrupp enligt Sats 31.1. Om $g \in G$ och $n \in \ker \theta$ så har vi att

$$\theta(gng^{-1}) = \theta(g)\theta(n)\theta(g^{-1}) = \theta(g)e_H\theta(g)^{-1} = \theta(g)\theta(g)^{-1} = e_H$$

och därmed ligger gng^{-1} i $\ker \theta$.

KVOTGRUPPER

Låt N vara en normal delgrupp till en grupp G. Låt G/N beteckna mängden av alla högersidoklasser (ekvivalent, vänstersidoklasser). Vi kan definiera en operation på G/N så att G/N blir en grupp med avssende på denna operation.

Exempel. Hur definierade vi operationen $\oplus$ på $\mathbb{Z}_n$?

$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$. $[0] = \{nk, k \in \mathbb{Z}\} = \langle n \rangle$ är en delgrupp till $\mathbb{Z}$ (med addition) och $[r] = \langle n \rangle + r$, $r \in \mathbb{Z}$, är både höger- och vänstersidoklasser till $\langle n \rangle$ i $\mathbb{Z}$.

Likheten $[a] \oplus [b] = [a+b]$ kan vi skriva om som

$$(\langle n \rangle + a) \oplus (\langle n \rangle + b) = \langle n \rangle + (a+b).$$

Låt Na och $Nb \in G/N$ (additivt: $N+a$ och $N+b \in G/N$). Vi definierar en operation i G/N enligt

$$Na * Nb = N(ab) \quad \text{(additivt : } (N+a) * (N+b) = N + (a+b))$$

Lemma. Operationen $*$ är väldefinierad, dvs om $Ng_1 = Ng_2$ och $Nh_1 = Nh_2$ så är $Ng_1h_1 = Ng_2h_2$.

Bevis.

$Ng_1 = Ng_2 \Rightarrow g_1 \in Ng_2 \Rightarrow g_1 = n_1g_2$ för något $n_1 \in N$.

$Nh_1 = Nh_2 \Rightarrow h_1 \in Nh_2 \Rightarrow h_1 = n_2h_2$ för något $n_2 \in N$. Därmed gäller att

$$g_1h_1 = n_1g_2n_2h_2 = n_1g_2n_2g_2^{-1}g_2h_2.$$

Eftersom N är en normal delgrupp får vi att $g_2n_2g_2^{-1} = n_3$ för något $n_3 \in N$ och

$$g_1h_1 = n_1n_3g_2h_2$$

med $n_1n_3 \in N$ vilket visar att $g_1h_1 \in Ng_2h_2$ varav $Ng_1h_1 = Ng_2h_2$.

Sats 22.1 (32.1). Låt G vara en grupp och låt N vara en normal delgrupp till G. Då bildar G/N en grupp med avseende på operationen $*$. Denna grupp kallas för **kvoten av G med H**.

Bevis. Associativitet: Låt g_1, g_2, $g_3 \in G$. Då

$$(Ng_1 * Ng_2) * Ng_3 = Ng_1g_2 * Ng_3 = N(g_1g_2)g_3 =$$
$$= Ng_1(g_2g_3) = Ng_1 * Ng_2g_3 = Ng_1 * (Ng_2 * Ng_3)$$

Elementet $Ne = N$ är ett identitetselement, ty om $g \in G$ så är

$$Ne * Ng = N(eg) = Ng \text{ och } Ng * Ne = N(ge) = Ng.$$

Elementet Ng^{-1} är en invers till Ng, $g \in G$, ty

$$Ng * Ng^{-1} = Ngg^{-1} = Ne \text{ och } Ng^{-1} * Ng = Ng^{-1}g = Ne.$$

Alltså är G/N en grupp.

Om G är ändlig så är $o(G/N) = [G : N]$.

Exempel. $\mathbb{Z}/\langle n\rangle = \mathbb{Z}_n$.

FUNDAMENTALA HOMOMORFISATSEN FÖR GRUPPER

Om $\theta : G \to H$ är en grupphomomorfi med $\ker\theta = K$ är

$$G/K \approx Im\theta.$$

Dessutom, om θ är surjektiv så är $G/K \approx H$.

Bevis. Vi definierar $\Phi : G/K \mapsto Im\theta$ enligt

$$\Phi(Ka) = \theta(a).$$

- Φ är väldefinierad, dvs $Ka = Kb \Rightarrow \theta(a) = \theta(b)$: om $Ka = Kb$ så gäller $a \in Kb$ och $a = kb$ för något $k \in K$, varav

$$\theta(a) = \theta(kb) = \theta(k)\theta(b) = e_H\theta(b) = \theta(b).$$

- Φ bevarar operation:

$$\Phi(Ka * Kb) = \Phi(Kab) = \theta(ab) = \theta(a)\theta(b) = \Phi(Ka)\Phi(Kb).$$

- Φ är bijektiv: Φ avbidar hela G/K på hela $Im\theta$ och därmed är surjektiv; Φ är injektiv, ty

$$\begin{aligned}&\Phi(Ka) = \Phi(Kb) \Leftrightarrow \theta(a) = \theta(b)\\ &(\text{ multiplicera med } \theta(a)^{-1} \text{ från höger})\\ &\Leftrightarrow e_H = \theta(b)\theta(a)^{-1} = \theta(b)\theta(a^{-1}) = \theta(ba^{-1})\\ &\Leftrightarrow ba^{-1} \in K(= \ker\theta) \Leftrightarrow b \in Ka \Leftrightarrow Kb = Ka.\end{aligned}$$

Alltså är Φ en isomorfi och $G/K \approx Im\theta$.

Exempel.

- $\langle n\rangle$ är en normal delgrupp till $\mathbb{Z}$ och kvoten $\mathbb{Z}/\langle n\rangle$ är $\mathbb{Z}_n$.
- $SL_n(\mathbb{R})$ är en normal delgrupp till $GL_n(\mathbb{R})$ och kvoten $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ är (isomorf med) $\mathbb{R}\setminus\{0\}$ (med multiplikation)

Vi har surjektiva homomorfier $\theta_1 : \mathbb{Z} \to \mathbb{Z}_n$ $(\theta_1(k) = [k],\ k \in \mathbb{Z})$ och $\theta_2 : GL_n(\mathbb{R}) \to \mathbb{R}\setminus\{0\} = \mathbb{R}^*$ $(\theta_2(A) = \det A,\ A \in GL_n(\mathbb{R}))$ med kärnor $\langle n\rangle$ respektive $SL_n(\mathbb{R})$.

Exempel. Definiera $\theta : \mathbb{Z}_{12} \to \mathbb{Z}_4$ enligt $\theta([a]_{12}) = [a]_4$.

1. θ är en väldefinierad avbildning dvs definitionen av denna avbildning beror inte på heltalet a som definierar kongruensklassen:

$$[a]_{12} = [b]_{12} \Leftrightarrow 12|(a-b) \Rightarrow 4|(a-b) \Rightarrow [a]_4 = [b]_4.$$

2. θ är en homomorfi:

$$\theta([a]_{12}\oplus[b]_{12}) = \theta([a+b]_{12}) = [a+b]_4 = [a]_4\oplus[b]_4 = \theta([a]_{12})\oplus\theta([b]_{12})$$

3. θ är surjektiv.

4. Kärnan $\ker\theta$ består av alla kongruensklasser $[a]_{12}$ sådana att $\theta([a]_{12}) = [0]_4$, dvs $[a]_4 = [0]_4$ vilket betyder att $4|a$. Vi får alltså

$$\ker\theta = \{[0]_{12}, [4]_{12}, [8]_{12}\} = \langle[4]_{12}\rangle.$$

Enligt homomorfi satsen är

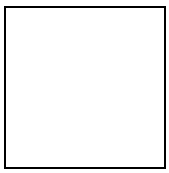
$$\mathbb{Z}_{12}/\langle[4]_{12}\rangle \approx \mathbb{Z}_4.$$

GRUPPVERKNINGAR

Exempel 1. Låt X vara en kvadrat i planet och låt G bestå av alla transformationer av planet som bevarar avståndet och kvadraten. G bildar en grupp med avseende på sammansättningen av två transformationer (Varför?). Denna grupp kallas ofta **kvadratgruppen**. G består i detta fall av följande 8 transformationer: 4 vridningar v_1, v_2, v_3, v_4: 0°, 90°, 180°, 270° kring kvadratens mittpunkt och 4 speglingar i linjerna s_1, s_2, s_3, s_4.

Man kan beskriva dessa transformationer med hjälp av följande permutationer av kvadratens hörn 1, 2, 3, 4:

$$\pi_{v_1} = (1), \pi_{v_2} = (1,2,3,4), \pi_{v_3} = (1,3)(2,4), \pi_{v_4} = (1,4,3,2)$$
$$\pi_{s_1} = (1,2)(3,4), \pi_{s_2} = (1,4)(2,3), \pi_{s_3} = (2,4), \pi_{s_4} = (1,3)$$



Sammansättningen av två transformationer motsvarar sammansättningen av respektive permutationer. Vi säger att G verkar på kvadratens hörn 1, 2, 3, 4.

Låt G vara en grupp och låt S vara en mängd. $Sym(S)$ betecknar gruppen av alla bijektiva funktioner med sammansättningen av funktioner som operation.

G **verkar på** S om det finns en grupphomomorfi

$$G \to Sym(S)$$

dvs att det till varje $g \in G$ kan man ordna en bijektiv funktion $\pi_g : S \to S$ så att

$$\pi_{gh} = \pi_g \circ \pi_h \quad \text{för alla } g, h \in G.$$

Exempel 2. En grupp verkar på sig själv på tre naturliga sätt:

(i) $\pi_g(h) = gh$, (multiplikation till vänster)
(ii) $\pi_g(h) = hg^{-1}$, (multiplikation till höger)
(ii) $\pi_g(h) = ghg^{-1}$ (konjugering)

Bevis. Övning.

BANOR

Om G verkar på S får vi en ekvivalensrelation på S genom

$$x \sim y \Leftrightarrow \pi_g(x) = y, \text{ för något } g \in G.$$

- Ekvivalensklasserna till denna relation kallas **banor** (x och y ligger i samma bana omm det finns $g \in G$ sådant att $\pi_g(x) = y$).
- Den bana som innehåller x betecknas $Orb(x)$.
- Om det finns bara en bana sägs G verka **transitivt**.

Exempel 3. Delgruppen $\{v_1, v_3\}$ av kvadratgruppen verkar på $S = \{1, 2, 3, 4\}$. Banorna är $Orb(1) = Orb(3) = \{1, 3\}$ och $Orb(2) = Orb(4) = \{2, 4\}$.

Delgruppen $\{v_1, v_2, v_3, v_4\}$ verkar på $S = \{1, 2, 3, 4\}$ med unik banan: $Orb(1) = Orb(2) = Orb(3) = Orb(4) = \{1, 2, 3, 4\}$.

STABILISATOR

För varje $s \in S$ bildar $G_s = \{g \in G : \pi_g(s) = s\}$ en delgrupp till G som kallas **stabilisatorn** till s.

Exempel. Om G är kvadratgruppen och $S = \{1, 2, 3, 4\}$ så är $G_1 = \{g \in G : \pi_g(1) = 1\} = \{v_1, s_3\}$, $G_2 = \{g \in G : \pi_g(2) = 2\} = \{v_1, s_4\}$, $G_3 = \{g \in G : \pi_g(3) = 3\} = \{v_1, s_3\}$, $G_4 = \{g \in G : \pi_g(4) = 4\} = \{v_1, s_4\}$.

Sats. Om en ändlig grupp G verkar på en mängd S och $s \in S$ så är

$$|Orb(s)| = [G : G_s] = \frac{|G|}{|G_s|}.$$

Bevis. Vi skall visa att elementen i $Orb(s)$ står i ett-ett-relation till sidoklasserna till G_s. För varje $s \in S$ har vi att

$$Orb(s) = \{\pi_g(s) : g \in G\}.$$

För g, $h \in G$ och $s \in S$ gäller att

$$\begin{aligned} \pi_g(s) = \pi_h(s) &\Leftrightarrow (\pi_h^{-1} \circ \pi_g)(s) = s \\ &\Leftrightarrow (\pi_{h^{-1}} \circ \pi_g)(s) = s \Leftrightarrow (\pi_{h^{-1}g})(s) = s \\ &\Leftrightarrow h^{-1}g \in G_s \Leftrightarrow g \in hG_s \Leftrightarrow gG_s = hG_s \end{aligned}$$

Detta ger att antalet olika element i $Orb(s)$ är lika med antalet olika sidoklasser till G_s. Därför är $|Orb(s)| = [G : G_s] = \frac{|G|}{|G_s|}$ enligt Lagranges sats.

ANTALET BANOR

Burnsides lemma. Om G är en ändlig grupp som verkar på en ändlig mängd S ges antalet banor av

$$\frac{1}{|G|}\sum_{g\in G}|\{s\in S:\pi_g(s)=s\}|.$$

Bevis. Vi räknar antalet element i mängden

$$X=\{(g,s)\in G\times S:\pi_g(s)=s\}\subseteq G\times S.$$

Detta kan göras på två olika sätt:

$$|X|=\sum_{g\in G}|\{s\in S:(g,s)\in X\}|=\sum_{g\in G}|\{s\in S:\pi_g(s)=s\}|$$

och

$$|X|=\textstyle\sum_{s\in S}|\{g\in G:(g,s)\in X\}|=\sum_{s\in S}|\{g\in G:\pi_g(s)=s\}|=$$
$$\sum_{s\in S}|G_s|=\sum_{s\in S}\frac{|G|}{|Orb(s)|}=\sum_{\text{banor}}|G|=|G|\cdot|\{\text{banor}\}|.$$

Exempel 4. På hur många olika sätt kan man måla en kvadrat med k färger om två färglägningar är lika om man får en av dem från den andra med hjälp av symmetriska transformationer?

Låt S vara mängden av alla färglägningar av en kvadrat med given orientering. Då är $|S|=k^4$.

Kvadratgruppen G verkar på S. Om $s\in S$ är en färglägning så består $Orb(s)$ av alla element som fås från s med hjälp av vridningar och speglingar. Därför är antalet olika färglägningar (två färglägningar är lika om man får en av dem från den andra med hjälp av symmetriska transformationer) lika med antalet banor då G verkar på S. Låt $\psi(g)=|\{s\in S:\pi_g(s)=s\}|$.

$\psi(v_1)=k^4$, ty v_1 är identiska transformationen och $\pi_{v_1}(s)=s$ för alla $s\in S$.

$\psi(v_2)=k$, eftersom en färgning s är invariant under v_2 omm alla sidor har samma färg.

$\psi(v_3)=k^2$, eftersom en färgning s är invariant under v_3 omm motsatta sidor ha samma färg.

$\psi(v_4)=k$ (samma argument som för v_2).

$\psi(s_1)=k^3$ (sidorna 14 och 23 måste ha samma färg).

$\psi(s_2)=k^3$ (samma argument som för s_1).

$\psi(s_3)=k^2$ (sidorna 12 och 14 måste ha samma färg och sidorna 23 och 34 måste ha samma färg).

$\psi(s_4)=k^2$ (liknande argument som för s_3).

Enligt Burnsides lemma får vi att antalet banor och därmed olika färglägningar är lika med $(k^4+2k+3k^2+2k^3)/8$.

Algebraiska strukturer, 25 februari

RINGAR

En mängd R med två binära operationer

$$(a,b) \mapsto a+b \text{ (addition)}$$
$$(a,b) \mapsto ab \text{ (multiplikation)}$$

är en **ring** om

- $(R,+)$ är en abelsk grupp,
- $a(bc) = (ab)c$, då a, b, $c \in R$ (multiplikation är associativ),
- $a(b+c) = ab+ac$ och $(b+c)a = ba+ca$ då a, b, $c \in R$ (multiplikation är distributiv m a p addition).

Anmärkning. Det neutrala elementet i gruppen $(R,+)$ brukar betecknas med 0. Vanligen säger man att R är en ring utan att använda beteckningen $(R,+,\cdot)$.

Exempel 1. (a) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ är ringar.
(b) $(\mathbb{Z}_n,\oplus,\odot)$ är en ring. Det enda egenskap som vi inte har visat är distributiviteten

$$\begin{aligned}[a]\odot([b]\oplus[c]) &= [a]\odot[b+c] = [a(b+c)] = [ab+ac] = \\ &= [ab]\oplus[ac] = [a]\odot[b]\oplus[a]\odot[c]\end{aligned}$$

för $[a]$, $[b]$, $[c] \in \mathbb{Z}_n$.
(c) Mängden, $M_n(\mathbb{R})$, av alla $n \times n$-reella matriser med matrisaddition och matrismultiplikation är en ring.
(d) Mängden, $\mathbb{Z}[\sqrt{2}]$, av alla tal av typen $a+b\sqrt{2}$ där a, $b \in \mathbb{Z}$. För att se detta räcker det att visa att mängden är sluten under vanlig addition och multiplikation:

$$(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2}) = (a_1+a_2)+(b_1+b_2)\sqrt{2} \in \mathbb{Z}[\sqrt{2}],$$
$$(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2}) = (a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1))\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

Låt $(R,+,\cdot)$ vara en ring.

- R är **kommutativ** om $ab = ba$ då a, $b \in R$.
- R har en **etta** om det finns ett neutralt element $1 \in R$ m a p multiplikation, dvs $1a = a1 = a$ då $a \in R$.

Exempel 2. (a) Alla ringar i Exempel 1 är kommutativa med undantag av $M_n(\mathbb{R})$ då $n \geq 2$.
(b) Alla ringar i Exempel 1 har en etta. Ett exempel på en ring utan etta är ringen av de jämna heltalen med vanlig addition och multiplikation.

Eftersom en ring R är en grupp m a p addition, så gäller följande:
(1) $a+b = a+c \Rightarrow b = c$, då a, b, $c \in R$,
(2) $a+x = b \Leftrightarrow x = b+(-a)$, då a, b, $x \in R$,

(3) $-(-a) = a$, $-(a+b) = (-a) + (-b)$, då $a, b \in R$,
(4) $(m+n)a = ma+na$, $m(a+b) = ma+mb$, $m(na) = (mn)a$ då $m, n \in \mathbb{Z}$ och $a, b \in R$.

Varning. $ab = ac \not\Rightarrow b = c$ och $ba = ca \not\Rightarrow b = c$ i allmänhet:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \text{ och } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

Låt R vara en ring, $a, b \in R$. Då
(1) $0 \cdot a = a \cdot 0 = 0$,
(2) $a(-b) = (-a)b = -(ab)$,
(3) $(-a)(-b) = ab$.

INTEGRITETSOMRÅDE OCH KROPPAR

- Låt R vara en kommutativ ring. Vi säger att R saknar **nolldelare** om $ab = 0$ ger $a = 0$ eller $b = 0$ då $a, b \in R$ (om $ab = 0$ där $a \neq 0$ och $b \neq 0$ så kallas a och b **nolldelare**).
- En kommutativ ring R kallas en **kropp** om $(R \setminus \{0\}, \cdot)$ är en abelsk grupp.
- Man säger att en ring R är ett **intgritetsområde** om R är kommutativ, saknar nolldelare och har en etta $1 \neq 0$.

Exempel 3. (a) Alla ringar i exempel 1 (a) saknar nolldelare. Men det finns nolldelare i t ex $\mathbb{Z}_6$: $[2] \odot [3] = [0]$. Ringen $M_2(\mathbb{R})$ har nolldelare ty t ex

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

(b) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ är exempel på kroppar. $\mathbb{Z}$ är inte kropp, eftersom $(\mathbb{Z} \setminus \{0\}, \cdot)$ inte är en grupp.
(c) Varje kropp K är ett integritetsområde ty $ab = 0$ och $a \neq 0$ ger att $a^{-1}(ab) = b = 0$, där $a, b \in K$ så att K saknar nolldelare. Klart att K har en etta $1 \neq 0$.

Proposition. $\mathbb{Z}_n$ är ett integritetsområde omm n är ett primtal.

Bevis. $\mathbb{Z}_n$ är en kommutativ ring med ettan $[1] \neq [0]$ då $n > 1$.

Om n inte är ett primtal dvs $n = n_1 n_2$ med $1 < n_1, n_2 < n$ så har $\mathbb{Z}_n$ nolldelare ty $[n_1] \odot [n_2] = [0]$ trots att $[n_1] \neq [0] \neq [n_2]$.

Om n är ett primtal så saknar $\mathbb{Z}_n$ nolldelare, ty $[s_1] \odot [s_2] = [0]$ med $0 \leq s_1, s_2 < n$ medför att $n | s_1 s_2$ varav $n | s_1$ eller $n | s_2$ vilket är möjligt omm $s_1 = 0$ eller $s_2 = 0$.

Kroppar $\subset$ Integritetsområde $\subset$ Kommutativa ringar $\subset$ Ringar

---

Exempel 4. $R = \mathbb{Z}$ är en kommutativ ring. R är ett integritetsområde. R är inte en kropp.

$\mathbb{Z}_6$ är en kommutativ ring men inte ett integritetsområde.

$M_2(\mathbb{R})$ är en icke-kommutativ ring.

Sats 25.1 (22.1) Låt D vara ett integritetsområde och a, b, $c \in D$, $a \neq 0$. Då gäller strykningarna: $ab = ac \Rightarrow b = c$.

Bevis. $ab = ac \Rightarrow a(b-c) = 0$. Eftersom D saknar nolldelare och $a \neq 0$ får vi att $b - c = 0$ och $b = c$.

Sats 26.1 (23.1) Varje ändligt integritetsområde är en kropp.

Bevis. Låt D vara ett integritetsområde. $D \setminus \{0\}$ är sluten under multiplikation, ty $ab = 0$ och $a, b \in D$ ger $a = 0$ eller $b = 0$. Multiplikationen är associativ på $D \setminus \{0\}$ ty den är associativ på hela D. D har en etta $1 \neq 0$. Vi måste visa bara att varje element $a \neq 0$ i D har en invers m a p multiplikation, dvs det finns b i D sådant att $ab = 1$. Vi fixar $a \neq 0$ i D och definierar en avbildning $\lambda_a : D \to D$ enligt

$$\lambda_a(x) = ax.$$

λ_a är injektiv, ty $ax = ay$ ger $x = y$ enligt Sats 25.1. Vi får då att $|\{\lambda_a(x) : x \in D\}| = |D|$. Eftersom D är ändlig och $\{\lambda_a(x) : x \in D\} \subseteq D$ har vi att

$$\{\lambda_a(x) : x \in D\} = D,$$

vilket ger att det finns $b \in D$ sådant att $\lambda_a(b) = 1$ dvs $ab = 1$. Alltså är $D \setminus \{0\}$ en grupp m a p multiplikation.

Följdsats. $\mathbb{Z}_n$ är en kropp omm n är ett primtal.

Bevis. Enligt Proposition 1 är $\mathbb{Z}_n$ ett integritetsområde omm n är ett primtal. Påståendet följer nu ur Sast 26.1.

DELRINGAR OCH DELKROPPAR

Man säger att S är en **delring** till en ring R om $S \subseteq R$ och elementen i S bildar en ring med avseende på operationerna i R.

Exempel. $(\mathbb{Z}, +, \cdot) \subset (\mathbb{Q}, +, \cdot) \subset (\mathbb{R}, +, \cdot) \subset (\mathbb{C}, +, \cdot)$.

Sats. En delmängd S till en ring R är en delring omm S är icke-tom, S är sluten under operationerna i R och $-a \in S$ för varje $a \in S$.

Man säger att en delmängd F till en kropp K är en **delkropp** till K om F är en kropp m a p operationerna i K.

ENHETER

Ett element $r \in R$ kallar man för en **enhet** om r har en multiplikativ invers dvs det finns $r' \in R$ så att $rr' = r'r = 1$. Mängden av alla enheter betecknas med R^*.

Exempel. $\mathbb{Z}$ har enbart två enheter ± 1. Varje element $a \neq 0$ i en kropp K är en enhet, ty $(K \setminus \{0\}, \cdot)$ är en grupp.

Sats. Gruppen av alla enheter i $\mathbb{Z}_n$ är $Z_n^* = \{[k] \in \mathbb{Z}_n : SGD(k, n) = 1\}$.

Bevis. Om $SGD(k, n) = 1$ så finns det heltal m och l sådana att $km + nl = 1$, varav $[k] \odot [m] = [1 - nl] = [1]$. Alltså är $[m]$ en invers till $[k]$.

Antag att $[k] \in \mathbb{Z}_n$ har invers $[m] \in \mathbb{Z}_n$ dvs $[k] \odot [m] = [1]$. Alltså är $km = 1 + nq$ för något heltal q. Den sista likheten visar att k och n saknar gemensamma delare $\neq 1$ dvs $SGD(k, n) = 1$.

Sats. Alla enheter i en kommutativ ring R med etta bildar en en (abelsk) grupp med avseende på multiplikation.

Bevis.=Övning

Algebraiska strukturer, 27 februari

PRODUKT AV RINGAR

Låt R_1, R_2,..., R_k vara ringar. Mängden

$$R_1 \times R_2 \times \ldots \times R_k$$

är en ring med avseende på koordinatvis addition och multiplikation dvs

$$(r_1, r_2, \ldots, r_k) + (r_1', r_2', \ldots, r_k') = (r_1 + r_1', r_2 + r_2', \ldots, r_k + r_k'),$$
$$(r_1, r_2, \ldots, r_k)(r_1', r_2', \ldots, r_k') = (r_1 r_1', r_2 r_2', \ldots, r_k r_k').$$

ISOMORFI AV RINGAR

Precis som för grupper är det intressant att veta vad man skall mena med att två ringar egentligen är samma ring.

Två ringar R och S är **isomorfa** om det finns en bijektion $\Phi : R \to S$ som uppfyller

- $\Phi(a + b) = \Phi(a) + \Phi(b)$, för alla a, $b \in R$.
- $\Phi(ab) = \Phi(a)\Phi(b)$, för alla a, $b \in R$.

På vänstra ledet är $+$ och $\cdot$ operationerna i R och på det högra ledet är $+$ och $\cdot$ operationerna i S.

Avbildningen Φ kallas då en **isomorfi av ringar** (eller **ringisomorfi**) och vi skriver $R \approx S$.

Eftersom en ringisomorfi $\Phi : R \to S$ är en isomorfi av abelska grupperna $(R, +)$ och $(S, +)$ så gäller följande:

- $\Phi(0) = 0$, $\Phi(-a) = -\Phi(a)$, $\Phi(ma) = m\Phi(a)$ då $a \in R$ och $m \in \mathbb{Z}$.

Exempel. $\mathbb{Z}_6 \approx \mathbb{Z}_2 \times \mathbb{Z}_3$.
Bevis. Betrakta $\Phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$, där $\Phi([a]_6) = ([a]_3, [a]_2)$.

- Definitionen av denna avbildning beror inte på heltalet a som definierar kongruensklassen (väldefinierad): Om $[a]_6 = [b]_6$ så är $[a]_3 = [b]_3$ och $[a]_2 = [b]_2$, ty $6|(a - b)$ implicerar att $3|(a - b)$ och $2|(a - b)$.
- Φ är injektiv, ty

$$\Phi([a]_6) = \Phi([b]_6) \Leftrightarrow ([a]_3, [a]_2) = ([b]_3, [b]_2) \Leftrightarrow$$
$$[a]_3 = [b]_3, [a]_2 = [b]_2 \Leftrightarrow 3|(a - b), 2|(a - b) \Rightarrow$$
$$6|(a - b) \Leftrightarrow [a]_6 = [b]_6$$

- Φ är surjektiv, ty Φ är injektiv och $|\mathbb{Z}_6| = |\mathbb{Z}_2 \times \mathbb{Z}_3| = 6$.
- Φ bevarar operationer:

$$\Phi([a]_6 + [b]_6) = \Phi([a + b]_6) = ([a + b]_3, [a + b]_2) =$$
$$= ([a]_3, [a]_2) + ([b]_2, [b]_3) = \Phi([a]_6) + \Phi([b]_6),$$
$$\Phi([a]_6[b]_6) = \Phi([ab]_6) = ([ab]_3, [ab]_2) =$$
$$= ([a]_3, [a]_2)([b]_2, [b]_3) = \Phi([a]_6)\Phi([b]_6)$$

Detta visar att Φ är en isomorfi.

KARAKTERISTIK

Låt R vara en kommutativ ring med ettan e. Vi säger att R har **karakteristik** n om n är den additiva ordningen av ettan i R, dvs om n är det minsta positiva heltal så att

$$ne = \underbrace{e + e + \ldots + e}_{n} = 0.$$

Om sådant n inte existerar säger vi att R har karakteristik 0. Karakteristiken av R kommer att betecknas med $\mathrm{char}(R)$.

Övning. Låt $\mathrm{char}(R) = n$. Visa att $na = 0$ för varje $a \in R$.

Exempel. (a) Ringarna $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ har karakteristik 0, ty $n1 \neq 0$ då n är ett positivt heltal.

(b) $\mathbb{Z}_n$ har karakteristik n, ty den additiva ordningen av [1] är n.

Sats 27.1 (24.1) Karakteristiken av ett integritetsområde är ett primtal eller 0.

Bevis. Låt D vara integritetsområde och låt e beteckna ettan i D. Antag att karakteristiken n är sammansatt, $n = pq \neq 0$. Då gäller

$$0 = ne = \underbrace{e + e + \ldots + e}_{n} = \underbrace{(e + e + \ldots + e)}_{p}\underbrace{(e + e + \ldots + e)}_{q} = (pe)(qe)$$

men eftersom D saknar nolldelare måste en av faktorerna vara noll, vilket motsäger minimaliteten hos n.

Sats 27.2,3 (24.2,3) Om ett integritetsområde har karakteristik $p \neq 0$ (respektive $p = 0$) innehåller D en delring K isomorf med $\mathbb{Z}_p$ (respektive $\mathbb{Z}$).

Bevis. 1. Låt $\mathrm{char}(D) = p \neq 0$. Låt $K = \{ke, k \in \mathbb{Z}\}$. Eftersom den additiva ordningen av e är p har vi att $|K| = p$. K är en delring till D (Varför?). Vi kan definiera en avbildning $\Phi : \mathbb{Z}_p \to K$ genom $\Phi([k]) = ke$, för alla heltal $k \in \mathbb{Z}$. Denna är väldefinierad, eftersom $[n] = [m]$ ger att $p|(n-m)$ dvs $n - m = qp$ för något $q \in \mathbb{Z}$, vilket visar nu att $ne - me = (n-m)e = qpe = 0$, dvs $me = ne$. Φ uppfyller $\Phi([m] + [n]) = \Phi([m]) + \Phi([n])$ och $\Phi([m][n]) = \Phi([m])\Phi([n])$, då $m, n \in \mathbb{Z}$. Φ är injektiv ty $\Phi([m]) = \Phi([n]) \Leftrightarrow \Phi([m-n]) = 0 \Leftrightarrow (m-n)e = 0 \Leftrightarrow p|m-n \Leftrightarrow [m] = [n]$. $|\Phi(\mathbb{Z}_p)| = p = |K|$. Alltså är K isomorf med $\mathbb{Z}_p$.

2. Låt $\mathrm{char}(D) = 0$. Övning.

POLYNOM

Ett **polynom** med koefficienter i en ring R kan vi se som ett formelt uttryck

$$a_0 + a_1 x + \ldots + a_n x^n,$$

där $a_0, a_1, \ldots, a_n \in R$.

Vi kan addera och multiplicera två polynom:

$$(a_0 + a_1x + \ldots) + (b_0 + b_1x + \ldots) = (a_0 + b_0) + (a_1 + b_1)x + \ldots$$
$$(a_0 + a_1x + \ldots + a_nx^n)(b_0 + b_1x + \ldots + b_mx^m) = c_0 + c_1x + \ldots + c_{n+m}x^{n+m},$$
$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

för $k = 0, 1, \ldots, m + n$. Mängden av polynom med koefficienter i R bildar en ring, $R[x]$-**polynomringen över** R. Om R är kommutativ blir $R[x]$ kommutativ.

Den **ledande termen** i $p(x) = a_0+a_1x+\ldots+a_nx^n$ är a_nx^n om $a_n \neq 0$. Då kallas a_n den **ledande koefficienten** och polynomets **grad** är n (grad $p(x)$). Vi antar att graden av nollpolynomet är -1.

Från och med nu förutsätter vi att K är en kropp.

Divisionsalgoritmen. Om $f(x)$ och $g(x)$ är polynom i $K[x]$, där K är en kropp, och $g(x) \neq 0$, finns det två entydigt bestämda polynom $q(x)$ och $r(x)$ i $K[x]$ så att

$$f(x) = q(x)g(x) + r(x)$$

och grad$r(x) <$ grad$g(x)$.

Bevis. Gör induktion över graden av $f(x)$ och eliminera den ledande termen i $f(x)$ med hjälp av $x^d g(x)$, där $d =$ grad$f(x) -$ grad$g(x)$.

Ett polynom med ledande koefficient 1 kallas **moniskt**.

Vi säger att $f(x)$ **delar** $g(x)$ i $K[x]$, eller $f(x)|g(x)$, om det finns ett polynom $h(x) \in K[x]$ så att $g(x) = f(x)h(x)$, dvs om resten vid division av $g(x)$ med $f(x)$ är noll.

Man säger att $a \in K$ är ett **nollställe** till $f(x) \in K[x]$ om $f(a) = 0$.

Faktorsatsen. Om $f(x) \in K[x]$ och K är en kropp, gäller att

$$(x - a)|f(x) \Leftrightarrow f(a) = 0$$

för alla $a \in K$.

Bevis. ($\Rightarrow$): Antag att $(x-a)|f(x)$. Då är $f(x) = (x-a)g(x)$ för något $g(x) \in K[x]$, och därmed $f(a) = (a - a)g(a) = 0$.

($\Leftarrow$): Antag att $f(a) = 0$. Använd divisionsalgoritmen för att skriva $f(x) = q(x)(x - a) + r(x)$, där grad$r(x) = 0$ eller $r(x) = 0$. Eftersom $f(a) = 0$ får vi $0 = q(a)(a - a) + r(a)$, och därmed $r(x) = 0$, eftersom $r(x)$ är ett konstant polynom.

Sats. Om $f(x)$ och $g(x)$ är polynom i $K[x]$, Kär en kropp, finns det ett unikt moniskt polynom $d(x)$ i $K[x]$ så att

(a) $d(x)|f(x)$ och $d(x)|g(x)$ och

(b) om $c(x)$ i $K[x]$ s.a. $c(x)|f(x)$ och $c(x)|g(x)$ så $c(x)|d(x)$.

Detta element kallas **största gemensamma delaren** till $f(x)$ och $g(x)$ ($SGD(f(x), g(x))$). Dessutom, finns det polynom $a(x)$ och $b(x)$ i $K[x]$ sådana att

$$SGD(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$

Satsen visas genom att utföra Euklides algoritm (precis som för heltal)

$SGD(f, g)$ är maximalt element (av högsta grad) bland de moniska gemensamma delarna till $f(x)$ och $g(x)$.

Algebraiska strukturer, 4 mars

REDUCIBLA OCH IRREDUCIBLA POLYNOM

Låt K vara en kropp. Ett icke-konstant polynom $f(x) \in R[x]$ är **irreducibelt över** R eller **irreducibelt i** $R[x]$ om det inte finns polynom $g(x)$ och $h(x)$ i $R[x]$ av grad större än noll så att $f(x) = g(x)h(x)$. Om $f(x) \in R[x]$ är icke-konstant polynom som inte är irreducibelt över R så kallas det **reducibelt över** K eller **reducibelt i** $R[x]$.

Exempel. (a) Varje polynom av grad 1 i $K[x]$ är irreducibelt.

(b) $x^2 + 2$ är irreducibelt i $\mathbb{R}[x]$, men reducibelt i $\mathbb{C}[x]$, ty $x^2 + 2 = (x - i\sqrt{2})(x + i\sqrt{2})$.

(c) varje polynom av grad 2 och 3 är irreducibelt i $K[x]$, där K är en kropp, omm det saknar nollställe i K: om $f(a) = 0$ så är $f(x) = (x - a)g(x)$ och grad $g(x) \geq 1$ varav $f(x)$ är reducibelt, omvänt om $f(x) = g(x)h(x)$ är en faktoruppdelning av $f(x)$ i två icke-konstanta faktorer så måste någon av dessa ha grad 1 och om $g(x) = b_0 + b_1 x$ så är $a = -b_0 b_1^{-1}$ ett nollställe till $g(x)$ och därmed till $f(x)$.

(d) (**Eisensteins kriterium**) Låt $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ vara ett polynom med heltalskoefficienter och låt p vara ett primtal sådant att $p|a_0, p|a_1, \ldots, p|a_{n-1}$, p inte delar a_n och p^2 inte delar a_0. Då är $f(x)$ irreducibelt över $\mathbb{Q}$.

UNIK FAKTORISERING AV POLYNOM

Lemma. Om $a(x)$, $b(x)$, $p(x) \in K[x]$, där K är en kropp, och $p(x)$ är irreducibelt så

$$p(x)|a(x)b(x) \Rightarrow p(x)|a(x) \text{ eller } p(x)|b(x)$$

Sats. Varje moniskt icke-konstant polynom i $K[x]$, där K är en kropp, kan skrivas som en produkt av ireducibla moniska polynom. Faktorisering är unik förutom ordningen av faktorerna.

Satsen och lemman bevisas på exakt samma sätt som motsvarande sats och lemma för heltalen.

Exempel. $x^4 - 4 = (x^2 - 2)(x^2 + 2)$ i $\mathbb{Q}[x]$,
$x^4 - 4 = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 2)$ i $\mathbb{R}[x]$,
$x^4 - 4 = (x - \sqrt{2})(x + \sqrt{2})(x + i\sqrt{2})(x - i\sqrt{2})$ i $\mathbb{C}[x]$.

UNIK FAKTORISERINGS OMRÅDE

$\mathbb{Z}$, $K[x]$, där K är en kropp, är standarta exempel på integritetsområde som har unik faktorisering: varje positivt heltal (moniskt polynom) kan skrivas som en produkt av primtal (respektive ireducibla moniska polynom) och sådan faktorisering är unik förutom ordningen av faktorerna.

I ett integritetsområde D säger vi att

- a **delar** b om det finns $c \in D$ så att $b = ac$
- a är en **enhet** om a delar 1 (a har en multiplikativ invers)

- $a \neq 0$ är irreducibelt om a ej är enhet och $a = bc$ innebär att antingen b eller c är en enhet.

Exempel. (a) Enheter i $\mathbb{Z}$ är ± 1. Irreducibla element är $\pm p$ där p är ett primtal.

(b) Enheter i en kropp K är $a \neq 0$, $a \in K$. Irreducibla element saknas.

(c) Enheter i $K[x]$ är konstanta polynom $\neq 0$. Irreducibla element är irreducibla polynom.

Vi säger att D har **unik faktorisering** om

- varje element $a \in D$ kan skrivas som en produkt av irreducibla element $a = p_1 p_2 \dots p_n$
- om $a \in D$ och $a = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$, där p_i, q_j är irreducibla så är $s = t$ och $p_i = e_i q_i$, där e_i är enheter, vid lämligt numerering av faktorerna.

Exempel. (a) $\mathbb{Z}, K[x]$, där K är en kropp, har unika faktorisering. ($24 = 2 \cdot 2 \cdot 3 \cdot 2 = (-2) \cdot (-3) \cdot 2 \cdot 2$. Här är $-2 = (-1) \cdot 2$, $-3 = (-1) \cdot 3$ och -1 är en enhet i $\mathbb{Z}$.

(b) $\mathbb{Z}[\sqrt{-3}] = \{a + ib\sqrt{3} : a, b \in \mathbb{Z}\}$ saknar unik faktorisering (i är den imäginära enheten).

Bevis. $\mathbb{Z}[\sqrt{-3}]$ är ett integritetsområde (Varför?).

Definiera $N : \mathbb{Z}[\sqrt{-3}] \to \mathbb{Z}^+$ ($\mathbb{Z}^+$ är mängden av icke-negativa heltalen) genom

$$N(a + ib\sqrt{3}) = |a + ib\sqrt{3}|^2 = a^2 + 3b^2.$$

N kallas en norm på $\mathbb{Z}[\sqrt{-3}]$ och uppfyller

- $N(z) \geq 0$ då $z \in \mathbb{Z}[\sqrt{-3}]$,
- $N(z) = 0$ omm $z = 0$,
- $N(z_1 z_2) = N(z_1)N(z_2)$ då z_1, $z_2 \in \mathbb{Z}[\sqrt{-3}]$.

Enheter i $\mathbb{Z}[\sqrt{-3}]$ är lösningar till $zw = 1$, $z, w \in \mathbb{Z}[\sqrt{-3}]$. Vi har att $zw = 1 \Rightarrow N(zw) = 1 \Leftrightarrow N(z)N(w) = 1$ och eftersom $N(z)$ och $N(w)$ är icke-negativa heltal blir den senare ekvivalent med $N(z) = N(w) = 1$, dvs enheter har normen 1. Vidare,

$$N(a + ib\sqrt{3}) = 1 \Leftrightarrow a^2 + 3b^2 = 1 \Leftrightarrow a = \pm 1, b = 0.$$

Klart att ± 1 är enheter i $\mathbb{Z}[\sqrt{-3}]$ och ± 1 är de enda enheter som finns i $\mathbb{Z}[\sqrt{-3}]$.

I $\mathbb{Z}[\sqrt{-3}]$ gäller att

$$4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$$

Om vi visar att 2 och $1 \pm i\sqrt{3}$ är irreducibla i $\mathbb{Z}[\sqrt{-3}]$ så visar vi att $\mathbb{Z}[\sqrt{-3}]$ saknar unik faktorisering.

Antag att $1 + i\sqrt{3} = xy$ där $x, y \in \mathbb{Z}[\sqrt{-3}]$. Då

$$4 = N(1 + i\sqrt{3}) = N(x)N(y)$$

vilket visar att $N(x) = 1, 2, 4$. Om $N(x) = 1$ så är x en enhet. Om $N(x) = 4$ så är $N(y) = 1$ och y är en enhet. Om $N(x) = 2$

och $x = a + ib\sqrt{3}$, $a, b \in \mathbb{Z}$, så är $a^2 + 3b^2 = 2$ vilket är omöjligt. Detta ger att $1 + i\sqrt{3} = xy$ gäller i $\mathbb{Z}[\sqrt{-3}]$ omm en av faktorerna är en enhet, dvs $1 + i\sqrt{3}$ är irreducibelt.

På ett liknande sätt visar man att $1 - i\sqrt{3}$ och 2 är irreducibla. Alltså saknar $\mathbb{Z}[\sqrt{-3}]$ unik faktorisering.

Varning! 13 är ej irreducibelt i $\mathbb{Z}[\sqrt{-3}]$ ty $13 = (1+i2\sqrt{3})(1-i2\sqrt{3})$, fast det är primtal och därmed är irreducibelt i $\mathbb{Z}$.

EUKLIDISKA OMRÅDEN

Ett integritetsområde D kallas Euklidiskt om det finns en funktion $d : D \setminus \{0\} \to \mathbb{Z}^+$ sådan att

- $d(\alpha\beta) \geq d(\alpha)$ då $\alpha \neq 0$, $\beta \neq 0$
- för α, $\beta \in D$ där $\beta \neq 0$ finns q och r så att

$$\alpha = q\beta + r \quad \text{med } d(r) < d(\beta) \text{ eller } r = 0$$

(Divisions algoritmen.)

Exempel. (a) $\mathbb{Z}$ är ett Euklidiskt område med $d(a) = |a|$.

(b) $K[x]$, där K är en kropp, är ett Euklidiskt område med $d(f(x)) = \text{grad } f(x)$.

Gaussiska heltalen. Låt $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, i är den imaginära enheten. Elementen i $\mathbb{Z}[i]$ kallas **Gaussiska heltalen**. $\mathbb{Z}[i]$ är ett integritetsområde.

Sats. $\mathbb{Z}[i]$ är ett Euklidisk område.

Bevis. Låt $d(a + bi) = |a + bi|^2 = a^2 + b^2$. Observera att för $z = a + bi \neq 0$ gäller att $d(a + bi) = a^2 + b^2 \geq 1$ och för z och w i $\mathbb{Z}[i]$ gäller

$$d(zw) = d(z)d(w) \geq d(z)$$

Det återstår att visa Divisions algoritmen. Låt α, $\beta \in \mathbb{Z}[i]$ med $\alpha = a_1 + a_2 i$, $\beta = b_1 + b_2 i$, $\beta \neq 0$. Vi måste hitta q och $r \in \mathbb{Z}[i]$ så att $\alpha = q\beta + r$ där $r = 0$ eller $d(r) < d(\beta)$. Vi skriver α/β på formen $\alpha/\beta = x + yi$, där x, $y \in \mathbb{Q}$. Låt q_1, q_2 vara heltal i $\mathbb{Z}$ så nära som möjligt till rationella talen x och respektive y. Låt $q = q_1 + q_2 i$ och $r = \alpha - q\beta$. Om $r = 0$ så är vi klara. Annars, har vi att $|x - q_1| \leq 1/2$ och $|y - q_2| \leq 1/2$ (enligt konstruktion av q). Detta ger

$$\begin{aligned}
&d(r) = d(\alpha - q\beta) = d(\beta(\alpha/\beta - q)) \leq \\
&d(\beta)d(\alpha/\beta - q) \leq d(\beta)d((x + yi) - (q_1 + iq_2)) \leq \\
&d(\beta)((x - q_1)^2 + (y - q_2)^2) \leq d(\beta)(1/4 + 1/4) < d(\beta).
\end{aligned}$$

Sats. Ett Euklidiskt område har unik faktorisering.

Algebraiska strukturer, 6 mars, 11 mars

HOMOMORFIER AV RINGAR

En avbildning $\Phi : R \to S$ mellan ringar kallas en **ringhomomotfi**, eller bara **homomorfi** om

- $\Phi(a+b) = \Phi(a) + \Phi(b)$ för alla $a, b \in R$.
- $\Phi(ab) = \Phi(a)\Phi(b)$ för alla $a, b \in R$.

Alltså är Φ speciellt en grupphomomorfi mellan de additiva grupperna i R och S ($\Phi(0_R) = 0_S$, $\Phi(-a) = -\Phi(a)$, $\Phi(na) = n\Phi(a)$, $\forall a \in R$).

En ringisomorfi = en bijektiv ringhomomorfi.

Exempel 1. Definiera $\Phi : \mathbb{Z} \to \mathbb{Z}_n$ genom $\Phi(k) = [k]_n$. Då är Φ en ringhomomorfi men ej isomorfi.

2. Definiera $\Phi : \mathbb{C} \to M_2(\mathbb{R})$ genom

$$\Phi(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Φ är en injektiv ringhomomorfi:

$$\Phi((a+ib)+(c+id)) = \Phi((a+c)+i(b+d)) =$$
$$\begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} =$$
$$\Phi(a+ib) + \Phi(c+id),$$

$$\Phi((a+ib)(c+id)) = \Phi((ac-bd)+i(ad+bc)) = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}$$
$$\Phi(a+ib)\Phi(c+id) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}$$

BILD OCH KÄRNA

Om $\Phi : R \to S$ är en ringhomomorfi ges **bilden** till Φ av

$$\Phi(R) = Im\Phi = \{\Phi(a) \in S \mid a \in R\}$$

och **kärnan** till Φ av

$$\ker \Phi = \{a \in R \mid \Phi(a) = 0_S\}$$

IDEAL

En delring I till en ring R är ett **ideal** om $ab \in I$ och $ba \in I$ för alla $a \in R$ och alla $b \in I$. Det betyder att I är invariant under multiplikation med alla element i ringen.

Exempel 1. $n\mathbb{Z}$ är ett ideal i $\mathbb{Z}$.
2. $\mathbb{Z}$ är ej ideal i $\mathbb{Q}$, ty $\frac{1}{2} \in Q$, $1 \in \mathbb{Z}$, men $\frac{1}{2} \cdot 1 \notin \mathbb{Z}$.

Sats 45.1. Låt $\Phi : R \to S$ vara en ringhomomorfi. Då gäller att

(i) $\Phi(R)$ är en delring i S.
(ii) $\ker \Phi$ är ett ideal i R.
(iii) Φ är injektiv omm $\ker \Phi = \{0_R\}$.

Bevis. Eftersom Φ är en grupphomomorfi mellan de additiva grupperna har vi att $\Phi(R)$ och $\ker \Phi$ är additiva delgrupper till $(S, +)$ respektive $(R, +)$. Det räcker nu att se på multiplikationen.

(i) Om $b = \Phi(a)$ och $b' = \Phi(a')$ i $\Phi(R)$ är

$$bb' = \Phi(a)\Phi(a') = \Phi(aa') \in \Phi(R)$$

dvs $\Phi(R)$ är sluten under multiplikation. Detta visar att $\Phi(R)$ är en delring i S.

(ii) Om $a \in R$ $b \in \ker \Phi \Leftrightarrow ab, ba \in \ker \Phi$, ty

$$\Phi(ab) = \Phi(a)\Phi(b) = \Phi(a)0_S = 0_S$$
$$\Phi(ba) = \Phi(b)\Phi(a) = 0_S\Phi(a) = 0_S$$

vilket visar att $\ker \Phi$ är sluten under multiplikation och därmed är en delring i R, och att $\ker \Phi$ är ett ideal.

(iii) samma som för grupper.

Varje element a i en ring R genererar ett ideal (a) (ett **huvudideal**, det minsta ideal som innehåller a) som består av alla element som kan skrivas $\sum_i b_i a c_i$ för b_i, c_i i R.

Om R är kommutativ , $a \in R$, så är

$$(a) = \{ra \mid r \in R\}.$$

Exampel. 1. Varje ideal i $\mathbb{Z}$ är ett huvudideal.

Bevis. Låt I vara ett ideal i $\mathbb{Z}$, $I \neq \{0\}$ och låt k vara det minsta positiva heltal som ligger i I. Då har vi att $km \in I$ för alla $m \in \mathbb{Z}$ och därmed $k\mathbb{Z} \subseteq I$. Antag att det finns $x \in I$ som inte tillhör $k\mathbb{Z}$. Enligt divisionsalgoritmen, $x = kq + r$, där $q, r \in \mathbb{Z}$ och $0 < r < k$. Eftersom $x \in I$, $kq \in I$, får vi att $x - kq = r \in I$ som strider mot minimalitetet av k. Därför $I = k\mathbb{Z} = (k)$.

2. Varje ideal i $K[x]$ är ett huvudideal (skall bevisas senare)

3. Om K är en kropp då saknar K icke-trivialla ideal I, dvs $I \neq \{0\}$, $I \neq K$.

Bevis. Om I är ett ideal, $I \neq \{0\}$, har I ett element $r \neq 0$. Då har vi att $r^{-1}r = 1 \in I$ (varje element $r \neq 0$ i en kropp har en invers) och $s \cdot 1 \in I$ för alla $s \in K$, som medför att $I = K$.

KVOTRINGAR

Låt I vara ett ideal i en ring R. Eftersom I är en delgrupp i den additiva gruppen i R kan vi definiera R/I som en abelsk grupp (med operation $+$: $(a+I)+(b+I)=(a+b)+I$).

Lemma. Om I är ett ideal i en ring R gäller att

$$a+I=c+I \text{ och } b+I=d+I \Rightarrow ab+I=cd+I.$$

Bevis. $a+I=c+I \Rightarrow (a-c)\in I$, och $b+I=d+I \Rightarrow (b-d)\in I$. Därmed gäller att

$$ab-cd=ab-ad+ad-cd=a(b-d)+(a-c)d$$

som ligger i I eftersom I är invariant under multiplikation med element i R.

Vi kan nu definiera en ringstruktur på R/I:

$(a+I)+(b+I)=(a+b)+I, \quad (a+I)\cdot(b+I)=ab+I,$ för alla $a,b\in R$.

Övning. Visa att R/I med de två operationerna är en ring. Denna ring kallas **kvoten av R med I**.

Exempel. $(n)=n\mathbb{Z}$ är ett ideal i ringen $\mathbb{Z}$ och kvoten $\mathbb{Z}/n\mathbb{Z}$ är $\mathbb{Z}_n$.

ISOMORFISATS

Om I är ett ideal i R finns en naturlig surjektiv homomorfi

$$\Phi : R \to R/I$$

genom $\Phi(a)=a+I$, för alla $a\in R$.

Sats. Om $\theta : R\to S$ är en ringhomomorfi då är

$$R/\ker\theta \approx \theta(R).$$

Bevis Definiera $\Phi : R/\ker\theta \to \theta(R)$ genom $\Phi(a+\ker\theta)=\theta(a)$. Eftersom vi vet att det är en isomorfi av abelska grupperna $(R/\ker\theta,+)$ och $(\theta(R),+)$ (se fundamentala homomorfisatsen för grupper) räcker det att visa att multiplikationen bevaras.

$$\Phi((a+\ker\theta)(b+\ker\theta))=\Phi(ab+\ker\theta)=$$
$$=\theta(ab)=\theta(a)\theta(b)=\Phi(a+\ker\theta)\Phi(b+\ker\theta).$$

KVOTRINGAR AV $K[x]$

Polynomet x^2+1 saknar nollställe i $\mathbb{R}$, men har ett nollställe i den större kroppen $\mathbb{C}$ ($\mathbb{R}\subset\mathbb{C}$). De komplexa talen fås från de reella talen precis genom att lägga till ett nollställe, som vi kallar i, till polynomet $x^2+1\in\mathbb{R}[x]$. Vi får se vidare att $\mathbb{C}\approx\mathbb{R}[x]/(x^2+1)$.

Om vi har något polynom som saknar nollställe i $K[x]$ kan vi uppfinna ett nollställe till polynomet genom att betrakta en ny

kropp L, som "innehåller" K och är av typen $K[x]/(p(x))$, där p är ett irreducibelt polynom i $K[x]$.

Sats 40.2 (47.2) Om K är en kropp, $p(x) = a_0 + a_1x + \ldots + a_nx^n$ är ett polynom av grad n i $K[x]$, och I är idealet $(p(x))$ i $K[x]$ så gäller att

(i) varje sidoklass kan skrivas entydigt som

$$I + (b_0 + b_1x + \ldots + b_{n-1}x^{n-1}),$$

där $b_0, b_1, \ldots, b_{n-1} \in K$.

(ii) $\{I + b : b \in K\}$ är en delkropp till $K[x]/I$ som är isomorf med K.

Bevis. (i) Låt $I + f(x) \in K[x]/I$. Enligt divisionsalgoritmen kan $f(x)$ skrivas som $f(x) = q(x)p(x) + r(x)$ med $q, r \in K[x]$, där $grad\ r(x) < grad\ p(x)$ eller $r(x) = 0$. Eftersom $f(x) - r(x) = q(x)p(x) \in I$ får vi att $f(x) \in I + r(x)$ och

$$I + f(x) = I + r(x).$$

Vidare,

$$I + (b_0 + b_1x + \ldots + b_{n-1}x^{n-1}) = I + (c_0 + c_1x + \ldots + c_{n-1}x^{n-1})$$

medför att

$$(b_0 - c_0) + (b_1 - c_1)x + \ldots + (b_{n-1} - c_{n-1})x^{n-1} \in I$$

och

$$(b_0 - c_0) + (b_1 - c_1)x + \ldots + (b_{n-1} - c_{n-1})x^{n-1} = 0,$$

ty alla nollskilda polynom $s(x)$ i I har grad större eller lika med $grad\ p(x) = n$. Alltså kan vi konstatera att $c_0 = b_0, \ldots, c_{n-1} = b_{n-1}$ och varje sidoklass i $K[x]$ kan representeras av exakt ett polynom $b_0 + b_1x + \ldots + b_{n-1}x^{n-1}$.

(ii) Betrakta funktionen $\Phi : \{I+b : b \in K\} \to K$, $\Phi(I+b) = b$, $b \in K$.

Anmärkning. Låt $p(x) \in K[x]$ och $I = (p(x))$. Då gäller att $I + f(x) = I + r(x)$, där $r(x)$ är resten vid division av $f(x)$ med $p(x)$.

Exempel. Ringen $\mathbb{R}[x]/(x^2 + 1)$ är isomorf med de komplexa talen $\mathbb{C}$.

Bevis. Varje sidoklass i $\mathbb{R}[x]/I$, där $I = (x^2 + 1)$, kan skrivas entydigt som $a+bx+I$, där $a, b \in \mathbb{R}$. Avbildningen $\Phi : \mathbb{R}[x]/I \to \mathbb{C}$ som ges av $\Phi(a + bx + I) = a + ib$ är väldefinierad eftersom alla sidoklasser i $\mathbb{R}[x]/I$ har en unik representant av grad högst 1. Vidare är den bijektiv och uppfyller

(i) om vi betecknar $a + bx + I = [a + bx]$, då är

$$\Phi([a + bx] + [c + dx]) = \Phi([(a + c) + (b + d)x]) = (a + c) + i(b + d) = (a + ib) + (c + id) = \Phi([a + bx]) + \Phi([c + dx])$$

(ii)

$$\Phi([a+bx]\cdot[c+dx]) =$$
$$\Phi(ac+(ad+bc)x+bdx^2+I) =$$
$$\Phi(ac-bd+(ad+bc)x+I) =$$
$$(\text{ty } bdx^2 = bd(x^2+1)-bd \in -bd+I) =$$
$$ac-bd+(ad+bc)i = (a+bi)\cdot(c+di) =$$
$$\Phi([a+bx])\Phi([c+dx]).$$

Alltså är $\mathbb{R}[x]/I$ isomorf med $\mathbb{C}$.

Polynomet x^2+1 har ett nollställe i $\mathbb{R}[x]/I$ (på grund av isomorfi $a \mapsto a+I$, $a \in \mathbb{R}$ skall koeficienterna a i polynomet interpreteras som $a+I=[a]$): $\alpha=[x]$ uppfyller $\alpha^2+[1]=[0]$, ty $[x]^2+[1]=[x^2+1]=[0]$.

Sats 40.1 (47.1) Om K är en kropp och $p(x) \in K[x]$ så gäller att $K[x]/(p(x))$ är en kropp omm $p(x)$ är irreducibelt i $K[x]$.

Bevis. Antag att $p(x)$ är irreducibelt och låt $I=(p(x))$. Antag att $g(x)+I \neq I$ dvs $g(x) \notin I$ vilket är ekvivalent att $p(x)$ inte delar $g(x)$.

Då är $SGD(p(x),g(x))=1$ och därmed finns det polynom $h(x)$, $l(x) \in K[x]$ så att

$$1 = SGD(p(x),g(x)) = p(x)h(x)+g(x)l(x).$$

Vidare är $1-g(x)l(x)=p(x)h(x) \in I$ och $g(x)l(x)+I=1+I$. Detta innebär att

$$(l(x)+I)(g(x)+I)=1+I.$$

Elementet $g(x)+I$ är alltså inverterbart med inversen $l(x)+I$.

Antag att $p(x)$ inte är irreducibelt och $grad\ p(x)>0$, dvs $p(x)=a(x)b(x)$, där $a(x)$, $b(x) \in K[x]$ är av $grad \geq 1$. Då är

$$a(x)b(x)+I=I$$

och därmed

$$(a(x)+I)(b(x)+I)=I$$

som medför att $a(x)+I$ är en nolldelare i $K[x]/I$. Alltså är $K[x]/(p(x))$ inte en kropp.

Om $grad\ p(x)=0$ eller $p(x)=0$ är $K[x]/(p(x))$ inte någon kropp heller (Varför?)

Sats 40.3 (47.3) Om K är en kropp så gäller att varje ideal i $K[x]$ är ett huvudideal.

Bevis. Låt I vara ett ideal i $K[x]$. Om $I=\{0\}$ då är det huvudideal. Låt $I \neq \{0\}$ och låt $p(x)$ vara ett polynom av minsta grad i I. Då är $p(x)q(x) \in I$ för varje $q(x) \in K[x]$ och därmed $(p(x)) \subset I$. Låt $f(x) \in I$. Enligt divisionsalgoritmen kan $f(x)$ skrivas som $f(x)=q(x)p(x)+r(x)$ där $q(x)$, $r(x) \in K[x]$ och $grad\ r(x) < grad\ p(x)$ eller $r(x)=0$. Eftersom $f(x)$, $q(x)p(x) \in I$ får vi att $f(x)-q(x)p(x)=r(x) \in I$ och därför $r(x)=0$, dvs $f(x) \in (p(x))$. Alltså är $I=(p(x))$.

SPLITTRINGSKROPP

Varje polynom med koeeficienter i en kropp kan uppdelas i förstagradsfaktorer i en lämlig utvidgning av denna kropp.

Sats. Låt K vara en kropp och $p(x)$ vara ett irreducibelt polynom. Då existerar en kropp $L \supseteq K$ sådan att p har ett nollställe i L.

Bevis. Låt $L = K[x]/(p(x))$ och $I = (p(x))$. Vi vet att L är en kropp och att den innehåller en delkropp som är isomorf med K så att vi kan identifiera varje element $I + b \in L$ med $b \in K$.

Låt $p(x) = a_0 + a_1x + \ldots + a_nx^n$ och låt α beteckna elementet $I + x \in L$. Då

$$p(\alpha) = a_0 + a_1(I + x) + \ldots + a_n(I + x)^n =$$
$$I + (a_0 + a_1x + \ldots + a_nx^n) = I + p(x) = I$$

vilket är noll i L.

Sats. Låt $p(x) \in K[x]$ och grad $p(x) \geq 1$. Då existerar en kropp $L \supseteq K$ sådan att p är en produkt av förstagradsfaktorer i $L[x]$.

Bråkkroppar av integritetsområden (se avsnitt 30 i Durbins bok)

Låt D vare ett integritetsområde och $D' = D \setminus \{0\}$. Vi skall bilda bråk med element i D som täljare och element i D' som nämnare. Vi studerar därför relationen $\sim$ på $D \times D'$ där $(a, b) \sim (c, d)$ om och endast om $ad=bc$.

Lemma 30.1 *Relationen ~ är en ekvivalensrelationen på* $D \times D'$

Bevis $\sim$ är reflexitiv då $ab=ba$ och symmetrisk eftersom $ad=bc \Rightarrow cb=da$. För transitiviteten, låt $(a, b) \sim (c, d)$ och $(c, d) \sim (e, f)$. Då är $ad=bc$, $cf=de$ och $(ad)f = (bc)f = b(cf) = b(de)$. Alltså gäller i så fall $d(af) = d(be)$. Men då D saknar nolldelare kan vi stryka $d \neq 0$, vilket ger att $(a, b) \sim (e, f)$.

Vi betecknar ekvivalensklassen av (a, b) m.a.p. $\sim$ med $\frac{a}{b}$ istället för $[a, b]$ som i kursboken. Vi kallar en ekvivalensklass $\frac{a}{b}$ för ett bråk med element i D. Observera att $b \neq 0$ för varje par (a, b) som representerar bråket.

Låt F_D vara mängden av alla bråk med element i D. Man definierar summan och produkten av två bråk enligt :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad , \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \quad .$$

Det är inte självklart att dessa operationer är väldefinierade och att högerleden är oberoende av de par (a,b) och (c,d) som representerar bråken. Men det följer av följande lemma.

Lemma 30.2 *Låt* $(a, b), (a', b'), (c, d), (c', d')$ *vara element i* $D \times D'$ *med* $\frac{a}{b} = \frac{a'}{b'}$ *och* $\frac{c}{d} = \frac{c'}{d'}$. *Då är* $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ *och* $\frac{ac}{bd} = \frac{a'c'}{b'd'}$.

För de binära operationerna + och $\cdot$ på F_D gäller följande resultat.

Lemma 30.3 *För ett integritetsområde D så är* $(F_D, +, \cdot)$ *en kropp med* $\frac{0}{1}$ *som nollelement och* $\frac{1}{1}$ *som etta. Den additiva inversen till* $\frac{a}{b}$ *är* $\frac{-a}{b}$ *och den multiplikativa inversen till* $\frac{a}{b} \neq \frac{0}{1}$ *är* $\frac{b}{a}$.

Kroppen F_D kallas *bråkkroppen* (eng. the field of fractions) *av D* eller *kvotkroppen* (eng. the field of quotients) *av D*. Om man talar om kvotkroppar är det viktigt att inte blanda ihop dessa med kvotringar *R/I*. De senare som bättre kallas restklassringar har inget med bråk att göra utan är en generaliserad kongruensräkning.

Lemma 30.4 *Låt D vara ett integritetsområde och* $\phi: D \to F_D$ *avbildningen där* $\phi(a) = \frac{a}{1}$. *Då är* ϕ *en injektiv ringhomomorfi.*

Ett integritetsområde D är alltså isomorft med delringen $\phi(D)$ av sin bråkkropp F_D. Man identifierar därför ofta D med sin bild $\phi(D)$ och ser D som en delring av sin bråkkropp.

Exempel 1 Bråkkroppen av ringen **Z** är kroppen **Q**. Den allmänna konstruktionen av bråkkroppar för integritetsområden är i själva verket modellerad på och en generalisering av konstruktionen av **Q**.

Exempel 2 Låt K vara en kropp och $D= K[x]$ vara ringen av alla polynom i x med koefficienter i K. Då är ett D ett integritetsområde. Dess bråkkropp F_D som skrives $K(x)$ kallas kroppen av rationella funktioner i x över K. Elementen i $K(x)$ är bråk $\frac{f(x)}{g(x)}$ av polynom i $K[x]$ där $g(x)$ är skilt från nollpolynomet. Om vi identifierar $K[x]$ med sin bild i $K(x)$ under ϕ så blir $K[x]$ en delring av $K(x)$ och K en delkropp av kroppen $K(x)$.

Exempel 3 Låt $D= \mathbf{Z}[i]$ vara ringen av Gaussiska heltal $a+bi$ där $a,b\in \mathbf{Z}$. Då kan bråkkroppen F_D av D identifieras med delkroppen av **C** bestående av alla komplexa tal $\alpha+\beta i$ där $x,y\in \mathbf{Q}$. För att se detta utnyttjar man följande identiteter i F_D :

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{(ad-bc)+(bc-ad)i}{c^2+d^2} = \frac{(ad-bc)}{c^2+d^2}+\frac{(bc-ad)}{c^2+d^2}\,\frac{i}{1}$$

Om vi låter $\alpha = \frac{(ad-bc)}{c^2+d^2}$ och $\beta = \frac{(bc-ad)}{c^2+d^2}$ kan vi alltså uppfatta $\frac{a+bi}{c+di}$ som det komplexa talet $\alpha+\beta i$.

Man kan gå vidare och konstuera en isomorfi från F_D till restklassringen $\mathbf{Q}[t]/(t^2+1)$ genom att avbilda $\alpha+\beta i$ på restklassen $\alpha+\beta t+(t^2+1)$ av det lineära polynomet $\alpha+\beta t \in \mathbf{Q}[t]$. Speciellt får vi då att $\mathbf{Q}[t]/(t^2+1)$ är en kropp vilket även följer av att polynomet t^2+1 är irreducibelt över **Q**.